DELJIS POLICIES AND PROCEDURES

POLICY: #4

TITLE: DELJIS ACCESS STANDARDS

APPROVED BY BOARD OF MANAGERS – DATE: 03/28/13
APPROVED BY: The Board of Managers
DATED SIGNED: 03/28/13
ORIGINAL EFFECTIVE DATE: 08/27/92
DISTRIBUTION:
REVISION DATE: 07/23/92; 05/25/00; 03/28/13

Section 8604 of Title 11 of the Delaware Code imposes a duty on the DELJIS Board of Managers to "ensure that the State Bureau of Identification and all other criminal justice agencies, collecting, storing, or disseminating criminal history record information and other information concerning crimes and offenders comply with Chapter 86 and Chapter 85 of Title 11." To do so, the Board is granted the authority "to promulgate rules and regulations to ensure compliance". (11 Del. C. § 8605).

Accordingly, the following rules and regulations (the "DELJIS Access Standards") are promulgated to ensure that the policies, procedures and guidelines related to accessing criminal justice data and the system conform to the statutory requirements outlined in Chapters 85 and 86 of Title 11 of the Delaware Code; to ensure that the data remains confidential; to ensure that the integrity of the data is not comprised; to ensure that the data remains secure; to ensure that the public trust in safeguarding the data is maintained; to provide a mechanism to guide ethical and responsible use; and to establish procedures and sanctions for the Board of Managers Executive Committee to impose when an individual uses the data improperly and without authorization. Access to the Delaware Criminal Justice Information System (DELJIS) is a privilege granted to an Authorized User by the DELJIS Board of Managers, it is not a guaranteed right of employment with an authorized Agency/Department.

I. Definitions

A. **Delaware Criminal Justice Information System:**

As defined by 11 Del. C. § 8602(4)

B. **Authorized Agency:**

A Criminal Justice Agency as defined by 11 Del. C. § 8505(d) or an approved Governmental Agency pursuant to 11 Del. C. § 8610 that has access to the Delaware Criminal Justice Information System.

C. **Authorized User:**

Any employee, intern, extern, contractor, volunteer or other individual who has direct or indirect access to CJIS or DMV data that is accessed via DELJIS acting on behalf of an authorized agency.

1. Types of access:

   a. Direct Access
   Access to CJI (Criminal Justice Information) via authorized and approved DELJIS credentials

   i.e., DELJIS user ID and password

   b. Indirect Access

   Access to CJI (Criminal Justice Information) and/or CHRI (Criminal History Record Information), in online or printed form as defined by 11 Del. C. § 8602(2), by authorized user(s) without approved DELJIS credentials for direct access.

2. **Improper Access/Breach:**

   Obtaining CJI or CHRI in either on-line or in printed form without a specific business reason directly related to the user's authorized access. This includes access for the purpose of confirming the existence or non-existence of CJI or CHRI. This also includes the transmission or non-transmission of said information obtained.

D. **CHRI (Criminal History Record Information)**

As defined by 11 Del. C. § 8602(2)

E. **CJI (Criminal Justice Information)**

Is the term used to refer to all of the DELJIS provided data necessary for law enforcement, other criminal justice, and any non-criminal justice or civil agencies who are authorized access to perform their missions. CJI includes but are not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets that fall into these categories:

1. Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

2. Identity History Data

Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

3. Biographic Data

Information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data

Information about vehicles and property as well as their owners. Such information may or may not be associated with a specific criminal report or investigation, but accessed as part of a user's need to fulfill their duties.

5. Case/Incident History

Information about the history of criminal incidents.

F. **Crime or Offense:**

As defined by 11 Del. C. § 233

G. **Dissemination:**

As defined by 11 Del. C. § 8602(6) and 11 Del. C. § 8502(8)

H. **Serious motor vehicle violation:**

Any violation of the motor vehicle code which is classified as a felony.

I. **Closed Session:**

A session of the Executive Committee which is not open to the public.

J. **Open Session:**

A session of the Executive Committee which is open to the public.

II. Responsibilities of Authorized Agencies

A. The head of an authorized agency must ensure Authorized Users within their Agency/Department complies with the DELJIS use requirements.

1. Authorized Agency/Department must submit a written request for access to the DELJIS Security Manager and shall obtain a fingerprint based criminal history report from SBI for each user.

2. The Agency/Department head or designee must ensure all users of said agency have read and signed a copy of this policy. (Attachment A) The agency shall be responsible for returning the signature page for each user to the DELJIS Security Manager.

3. The Agency/Department head or designee shall certify for completeness and accuracy a list of users provided annually from DELJIS to the agency head. The list shall be certified as is, or corrected to delete, add or change users and returned to DELJIS within 60 days of receipt of said list by the Agency/Department head or designee.

4. The Authorized Agency/Department is responsible for notifying DELJIS immediately upon a user's departure (transfer, termination, resignation, or retirement) from said Agency/Department.

5. The Authorized Agency/Department is responsible for notifying DELJIS immediately upon an employee's suspension or administrative leave from the Agency/Department, if the suspension or administrative leave

exceeds 24 hours or results in loss of agency privileges, identification, credentials or departmental weapon.

6. Agency/Department head or designee shall report all notices of a user's arrest, charge(s), or conviction of a criminal violation or offense in any jurisdiction to DELJIS immediately upon receiving notification themselves.

7. The DELJIS Security Manager will conduct an Agency/Department site inspection when required to ensure physical site suitability and security.

8. The Agency/Department head or designee is responsible for ensuring all Agency/Department users attend the appropriate amount of DELJIS training.

III. Responsibilities of Authorized Users

A. Authorized Users must hold themselves to the highest standards and must conduct themselves in a manner that will ensure the security, integrity and confidentiality of the data contained within the CJI systems.

1. Authorized Users shall not improperly access information contained within the CJI system for any reason other than authorized work related reasons.

2. Authorized Users must read and sign a copy of DELJIS Policy #4 and annually acknowledge. (Attachment A).

3. Authorized Users are required to read and submit a DTI (Department of Technology and Information) Acceptable Use Policy. (Attachment B).

4. Authorized Users must complete DELJIS provided training prior to being granted a user credential.

5. Authorized Users/Agencies shall be required to maintain secondary dissemination logs; per 11 Del. C. § 8513(e), by all Agency/Departments disseminating CHRI.

6. Authorized Users who become aware of improper access of CJIS by another user, or by any other entity, shall report the violation(s) to their Agency/Department Head, Management or directly to DELJIS immediately.

7. Authorized Users who have been arrested, charged, or convicted of a criminal offense or violation in any jurisdiction, shall notify their Agency/Department Head or Management within 24 hours of the arrest, charge, or conviction.

8. Authorized Users who have been arrested, charged, or convicted of a serious motor vehicle offense (as defined by DELJIS Policy 4 Section "I", subsection "H") in any jurisdiction, shall notify their Agency/Department Head or Management within 24 hours of the arrest, charge, or conviction, or directly to DELJIS within the same period of time.

IV. Denial of DELJIS Access Upon Initial Application

A. To determine if access should be granted for a requesting Agency/Department, the DELJIS Board of Managers will consider whether the Agency/Department has;

1. justifiable needs per 11 Del. C. § 8513A, which outlines the process for requesting access to DELJIS.

B. To determine if access should be granted for an individual, the Executive Director and/or the DELJIS Board of Managers may consider whether the individual has:

1. been charged with or convicted of a criminal offense or serious motor vehicle violation;

2. an active warrant or capias;

3. an active Protection from Abuse Order or Protection Order entered against him/her;

4. intentionally falsified any official record;

5. improperly accessed CJIS previously;

6. engaged in any other activity which could endanger the security, privacy or integrity of CJIS.

C. Denial Procedure

1. The Executive Director makes the initial determination to deny access.

2. A notification of denial of access will be sent to the Agency/Department Head or Management.

3. Agency/Department Head may appeal the denial to the Executive Committee of the Board of Managers:

   a. the appeal must be made within 5 days of the Agency/Department Head or Management receiving initial Notice of Denial.

   b. the appeal must be in writing via email, fax or U.S. Mail to the attention of the Chairperson of the Executive Committee of the Board of Managers.

V. Suspension/Termination of DELJIS Access

A. Process regarding notification of a Warrant, Arrest or/Conviction by a DELJIS Authorized User,

1. Upon notification of an arrest/conviction or upon the discovery of an Authorized User's arrest/conviction for:

   a. a criminal offense, violation or,

   b. a serious motor vehicle offense.

   The Executive Director of DELJIS will make the initial determination if the charge(s) warrant an immediate suspension of said User's CJIS access:

2. If the Executive Director's determination does not suspend the DELJIS User's access; no action will be taken to the User's access.

3. If the Executive Director's determination suspends the DELJIS User's access, the access will be suspended immediately by the DELJIS Security Manager and/or designee:

   a. the Executive Director will inform the Executive Committee of the facts concerning the arrest/conviction at their next regular

meeting.

4. After the Executive Director makes the initial determination to suspend the DELJIS User's access, the DELJIS Security Manager or designee will notify the Agency/Department Head or their designee via written notification, email, fax or U.S. Mail which outlines the following:

   a. name of DELJIS User who was arrested/convicted;

   b. date and time of the arrest and or conviction; and,

   c. the DELJIS User's right of appeal to the Executive Committee of the Board of Managers, within 5 calendar days of receipt of the notification.

      1. Failure to appeal the temporary suspension will result in the suspension remaining in effect until the arrest and/or conviction is resolved.

      2. The Executive Committee's decision of a temporary suspension is final and is not subject to further appeal or review.

5. It will be the Agency/Department Head's or their designee's responsibility, to ensure a copy of the suspension notification is delivered to the DELJIS User, their employee. The Agency/Department Head will then:

   a. notify DELJIS via notification or email confirming the suspension notification has been delivered to their employee; and,

   b. document the date, time and name of person who delivered the notification to the employee (DELJIS User) in question.

B. Process regarding notification of a violation of DELJIS policies i.e.; Improper Access, Improper Dissemination, and/or Unauthorized Use by a DELJIS Authorized User:

1. Upon notification of a violation of DELJIS policies or upon the discovery of a violation of DELJIS policies by an Authorized User involving:

   a. improper access;

   b. dissemination;

   c. unauthorized use; or,

   d. any other violation regarding DELJIS policies.

   The Executive Director of DELJIS will make the initial determination if the complaint/violation(s) warrant an immediate suspension of said Authorized User's CJIS access.

2. If the Executive Director's determination does not suspend the DELJIS User's access, no action will be taken to the User's access.

3. If the Executive Director's determination is to suspend the DELJIS User's access, the access will be suspended as soon as practicable by the DELJIS Security Manager and/or designee:

   a. the Executive Director will inform the Executive Committee of the facts concerning the arrest/conviction at their next regular meeting.

4. After the Executive Director makes the determination to suspend the DELJIS User's access, the DELJIS Security Manager and/or designee will notify the Agency/Department Head or designee via written notification, email, fax, or U.S. Mail, the notification will contain the following Information:

   a. name of DELJIS User, who is suspected of the violation; and,

   b. the alleged violation(s) of DELJIS policies.

   c. This temporary suspension of DELJIS access cannot be appealed unless:

1. the investigation will take longer than 30 days to complete or,

2. the suspension creates an undue operational hardship on the agency as a whole.

d. If (IV.B.4.c.1 or IV.B.4.c.2) occurs, the temporary suspension may be appealed to the Executive Committee of the DELJIS Board of Managers, within 5 calendar days of receipt of the notification.

5. The Executive Director will authorize an investigation into the DELJIS User's access of the system regarding the allegations or allegations concerning DELJIS policies.

6. It will be the Agency/Department Head's or their designee's responsibility to ensure a copy of the suspension notification is delivered to the DELJIS User, their employee. The Agency/Department Head will then:

a. notify DELJIS via notification or email confirming the suspension notification has been delivered to their employee; and,

b. document the date, time and name of person who delivered the notification to the employee (DELJIS User) in question.

VI. Procedure for Conducting the Administrative Investigations

A. The DELJIS investigator will conduct an the administrative investigation as a civilian, on behalf of the Executive Committee of the DELJIS Board of Managers, for all DELJIS users except those listed in VI B.

B. If the complaint involves allegation(s) which involve members of the Delaware State Police, the investigation will be handled by a sworn member of the Delaware State Police assigned to SBI (State Bureau of Identification).

1. The DSP investigator shall present the facts of the investigation to the Executive Committee personally or provide sufficient facts to either the DSP Board representative and/or the DELJIS investigator who will then present the facts of the investigation to the Executive Committee on be half of the DSP investigator.

C. If an authorized agency/department conducts its own internal investigation to supplement the DELJIS investigation, on its user regarding possible DELJIS policy

violations, the agency/department must provide sufficient facts as they pertain specifically to the DELJIS policy violations to the Executive Director of DELJIS or to the Executive Committee of the DELJIS Board of Managers. An agency supplemental investigation can be submitted to DELJIS in writing.

D. The DELJIS and or DSP investigator will schedule a date and time to interview the individual at a mutually agreed upon location.

E. The individual interviewed may elect to have his/her attorney, or union representative present during the interview. Only the employee or the attorney will be permitted to speak during the interview.

1. The interviews will be conducted in a respectful, non-hostile and or non-aggressive manner.

2. The interviews will be audio recorded whenever possible.

F. At the conclusion of the interview, the DELJIS or DSP investigator will advise the individual of the possible sanctions which may be imposed by the Executive Committee of the DELJIS Board of Managers and also that the Delaware Department of Justice will review the facts of the investigation to determine if criminal prosecution is warranted.

1. If a criminal investigation is deemed appropriate a separate investigation will be conducted by a law enforcement agency.

G. The DELJIS or DSP investigator will complete a written LEISS report detailing the facts concerning the investigation.

1. The DELJIS investigator's report will be approved by the Executive Director of DELJIS, or

2. The DSP investigator's report will be approved by the supervisor of the DSP officer who investigated the complaint.

H. At the conclusion of the investigation and prior to the investigation being presented to the Executive Committee, the facts of the administrative investigation will be submitted to the Attorney General's office to determine if there was any violation of the Delaware Code warranting criminal prosecution.

1. If a criminal investigation is deemed appropriate, a separate investigation will be conducted by a law enforcement agency

I. The facts of the investigation will be presented to the Executive Committee of the DELJIS Board of Managers at their next regularly scheduled meeting unless circumstances dictate the Executive Committee act more expeditiously.

J. The Executive Committee of the DELJIS Board of Managers will then render their decision based on the preponderance of the information presented.

K. The Executive Committee may impose any sanction(s) deemed appropriate to the investigation, including but not limited to:

1. execute DELJIS Policy #4 and sign written acknowledgement;

2. retrain on the DELJIS system, specifically the security training;

3. cause the agency/department employee to log all of their CJIS transactions for a specific period of time. The log will be provided by DELJIS and once completed will be faxed to the DELJIS Security Manager or designee based on the time line imposed by the Executive Committee of DELJIS Board of Managers;

4. agency/department employee's usage monitor for a specific period of time. The DELJIS Security Manager or designee may contact the employee at any time requesting justification as to why the employee accessed a specific record;

5. suspend the user's access for a specific period of time;

6. suspend the user's access permanently; or,

7. assess reasonable fees for the recovery of the administrative cost of the investigation imposed against the employer of the investigated user.

L. Failure to comply with imposed sanctions will result in continued suspension from system.

M. Sanctions imposed by the Executive Committee of the DELJIS Board of Managers which have time constraints imposed shall be in effect as long the user has access to the CJI system.

1. Time when a user is on leave (Extended Leave, Suspended from Agency/Department, Family Medical Leave, Termination, and/or Resignation) will not count towards the time constraints imposed by the

Executive Committee unless approved by the Executive Director.

VII. Procedure for Conducting Administrative Investigations

A. An investigation is conducted and presented to the Executive Committee of the DELJIS Board of Managers.

B. The Executive Committee of the DELJIS Board of Managers imposes one or more of the sanctions listed under section (Section VI, subsections K1 to K7).

C. The DELJIS Security Manager and or designee will send a notification to the Agency/Department Head or designee, advising of the sanctions which were imposed by the Executive Committee of the DELJIS Board of Managers.

1. It will be the Agency/Department Head's or his designee's responsibility, to ensure a copy of the suspension notification is delivered to the DELJIS User, their employee. The Agency/Department Head or designee will then:

a. the appeal must be in writing via email, fax or U.S. Mail to the attention of the Chairperson of the Executive Committee of the Board of Managers

b. documenting the date, time and name of person who delivered the notification to the employee (DELJIS User) in question.

D. If the DELJIS User does not concur with the sanctions imposed against them by the Executive Committee, the DELJIS User has the right to appeal the Executive Board's decision.

VIII. Procedure for Pursuing an Appeal of an Administrative Decision

A. The DELJIS User has the right to appeal in writing to the Executive Committee within 5 calendar days of receiving the notification advising of the sanctions imposed by the Committee. The appeal notification should be sent to the DELJIS office.

B. The Appeal Hearing shall be scheduled for the next regular Executive Committee meeting unless circumstances require an earlier date be scheduled.

1. A notification will be sent to the Agency/Department Head or designee advising of the date and time of the hearing; and,

2. the Agency/Department Head or their designee will ensure the accused DELJIS User receives a copy of this notification.

C. The Appeal Hearing will be held in a "closed session". The DELJIS User may be accompanied by their lawyer, union representative or other persons the DELJIS User believes has relevant information to present to the Executive Committee.

D. The DELJIS User may present facts relating to their circumstances to challenge the final decision and / or the sanctions imposed by the Executive Committee.

E. At the conclusion of the DELJIS User's presentation, the Executive Committee will deliberate in closed session prior to announcing their decision. Once the Executive Committee reaches their decision, the DELJIS User will be advised of the Committee's decision in an "open session" of the Executive Committee;

1. The decision of the Executive Committee regarding the Appeal hearing will be referenced only by case number

2. Executive Committee's actions are subject to confirmation at the next Board of Managers meeting.

F. Once an appeal has been heard by the Executive Committee of the DELJIS Board of Managers, their decision is final and there is no appeal.

1. the Executive Committee's actions are subject to confirmation at the next Board of Managers meeting.

2. any decision affecting a DELJIS user may only be reviewed through a writ of certiorari to the Superior Court of Delaware.

STATE OF DELAWARE
DELAWARE CRIMINAL JUSTICE INFORMATION SYSTEM (DELJIS)
802 Silver Lake Boulevard
Suite 101
Dover, Delaware 19904
Telephone: 302-739-4856 Fax: 302-739-6285

March 28, 2013

TO: All Criminal Justice Information Users

REF: DELJIS Policy #4 Verification of Acknowledgement; Employee Access Standards

1. All criminal justice agencies will ensure that all requests for criminal justice information access will be channeled through the proper authorities as outlined in DELJIS Policy #4.

2. All agencies with approved criminal justice information access (Direct or Indirect Access) shall ensure that anyone within their agency/department shall be fingerprinted pursuant to DELJIS Policy #4 regarding the fingerprinting of employees.

3. It is the responsibility of the agency/department head or designee to ensure that all employees shall have read Policy #4. The agency/department shall be responsible for returning the signed "DELJIS Policy #4 Verification of Acknowledgement" and "DTI Acceptable Use Policy" to the DELJIS Security Manager or designee.

4. The agency/department shall notify the DELJIS Security Manager or designee immediately of the transfer, suspension, or termination of any employee having DELJIS access.

5. On an annual basis, each DIRECT and INDIRECT ACCESS Users will read DELJIS Policy #4 and verify acknowledgement on-line.

6. Anyone who fails to verify on-line on an annual basis, the DELJIS Security Manager will supply each agency/department with a listing of DIRECT and INDIRECT USERS for verification. The agency/department will be responsible for reviewing the list for compliancy and supply DELJIS with any additions, changes and/or deletions within 30 days and either have the users electronically sign or submit the signed forms to DELJIS.

Complete information on right if available or known.

SBI Number: _____
Agency Code: _____
Menu Option Level: _____
Logon ID: _____

****

DELJIS POLICY #4
VERIFICATION OF ACKNOWLEDGEMENT

_____ _____
Printed Full Name *Date of Birth*

☐ **Civilian** ☐ **Sworn Police Officer**

_____ _____
Sex *Race*

_____ _____
Other Names Used (Maiden, alias) *Driver License Number & State*

_____ _____
Agency (PLEASE PRINT) *County of Employment*

Email address: _____

THIS IS TO VERIFY THAT I HAVE READ AND UNDERSTAND DELJIS POLICY #4.

_____ **DATE:** _____
Employee's signature

****

Verifying Person:

_____ **DATE:** _____
Agency Head or Designee Signature

_____
Printed Name

Do you require a @cj.state.de.us email account (non-state employees): ☐ **Yes** ☐ **No**

Type of Access*: ○ **Indirect**

*Check the ones that apply. Indirect for no online access. Direct, select required access if known

○ **Direct Access**

- ○ **Inquiry**
- ○ **LEISS Complaint only**
- ○ **LEISS Print/Preview**
- ○ **Wanted Person Update**
- ○ **Update/Input**
- ○ **Police Officer**
- ○ **Dispatcher**
- ○ **Other (such as DACS, DUI Tracking, IT person only)**

○ **SSL/VPN (Agency head or designee contact DELJIS at 302-739-4856 for spreadsheet request form)**

PLEASE RETURN TO: Delaware Criminal Justice Information Systems
802 Silver Lake Boulevard, Suite 101
Dover, DE 19904
State Location Code: D530A
Fax: 302-739-6285

Rev: 03/28/2013