Division of Youth Rehabilitative Services

Chapter 2: Professional Practices

<table>
<thead>
<tr>
<th>Subject: Dissemination of DELJIS Criminal History Record Information (CHRI)</th>
<th>Policy # 2.15</th>
<th>Page: 1 of 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards: DELJIS Policies and Procedures</td>
<td>Policy #4</td>
<td></td>
</tr>
</tbody>
</table>

Effective Date: 10/22/10

Revised: 5/1/14

I. PURPOSE: To provide instruction on the dissemination and treatment of CJIS information.

II. POLICY: All information in CJIS is under the strict policy set by the agency known as the Delaware Criminal Justice Information System (DELJIS). All Division staff shall be in compliance with DELJIS policy at all times.

III. DEFINITIONS:

A. Direct Access: All direct care treatment supervisors and managers and other positions required by job responsibilities must have a User I.D. and Password to gain direct access.

B. Indirect Access: Access to Criminal Justice Information and/or 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. All DYRS employees are required at a minimum to have indirect access.

C. Criminal History Record Information (CHRI): Information collected by criminal justice agencies on an individual consisting of descriptions of the individual together with notes of arrests, detentions, indictments, information, or other formal charges, as well as dispositions, sentencing, and correctional supervision and release arising from those charges. CHRI does not include wanted posters, original entries on police blotters, Court records of judicial proceedings, published Court opinions or proceedings, or announcements of clemency.

D. Dissemination: The transmission of CHRI or the confirmation of the existence or non-existence of a criminal record.

IV. PROCEDURES:

A. Policy Acknowledgement: All DYRS employees must read and sign a Policy 4 form annually (http://server.deljis.state.de.us/deljis/pdfs/policyfour). This form must be signed regardless of whether the employee has a CJIS logon. Signed forms are to be returned to the DYRS FACTS Liaison who will forward them directly to DELJIS. These signed copies are also kept on file by the DYRS FACTS Liaison.
B. Logons: Before an employee is allowed a CJIS logon, a security clearance supported by fingerprints must be obtained. DELJIS will perform a thorough criminal history check and will contact the FACTS Liaison with any issues. Yearly, DELJIS will supply DYRS with a listing of all authorized users. DYRS (via FACTS Liaison) will review the list and supply any missing information such as missing forms, additions, changes, or deletions.

C. Employee Hiring: The following protocols must be followed when making a selection for hire:

1. Offers of employment are contingent upon receipt of a criminal background check, drug screen, and authorization for DELJIS access.
2. The transfers or promotion of Department or State employees that are not fingerprinted a second time, must be told of the need to be DELJIS approved for any position that requires a direct or indirect access to information obtained from DELJIS.

D. Employee Transfers, Resignations or Terminations:

1. The supervisor of any employee that transfers to another agency, resigns from employment or is terminated must report this action to the DYRS FACTS Liaison via an email. In turn, DELJIS will be notified to terminate their access.

E. DELJIS Suspension for Employee Disciplinary Action or Arrest:

1. The supervisor of any employee that is placed on suspension or administrative leave for more than twenty-four (24) hours must report this action to the DYRS FACTS Liaison via an email. In turn, DELJIS will be notified and the staff’s access to DELJIS and CJIS through FACTS will be suspended during this period. Notification for planned suspensions or administrative leave must be submitted immediately to the liaison.
2. If the suspension is due to employee arrest, the employee is responsible for providing final disposition and documentation. It is the employee’s responsibility to apply for reauthorization of DELJIS access when arrest has been disposed. DYRS is required to reactivate the logon upon reauthorization from DELJIS.
3. If reauthorization is denied for Direct or Indirect Access, the employee will be subject for termination.
4. Any employee that is restricted from access but fails to comply with the imposed sanction, i.e., accessing criminal justice information indirectly will result in continued restriction from the system.
5. Any employee that is restricted from access to the State's network but fails to comply or tries to access unauthorized State services or goods will be subject to disciplinary action.

F. Dissemination Rules: No person may disseminate CHRI except under the following conditions:

1. Employees of the same agency may disseminate to each other as long as both have access to DELJIS information.
2. CHRI may be disseminated to the State Bureau of Identification.
3. CHRI can be transmitted to another criminal justice agency for use in criminal justice proceedings.
4. CJIS viewed data pertains to DYRS clients and their family or household members. The latter viewing is for safety and rehabilitation purposes. Dissemination applies ONLY to Court ordered juvenile clients.
5. The dissemination may be by spoken word, copy of the documents from Court or printed from CJIS.
6. The document types include rap sheets, significant petitions (or exhibits if petitions are not created), warrants, adjudications, and dispositions.
7. The required information may include information about non-adjudicated charges.

G. Storage and Transmission of CHRI and CJIS Information: (this information does not apply to paperwork given to us by the Courts.

1. Any information copied, pasted, or printed must be secured in the client’s file and shredded upon closure of the case. The printed CHRI must not be viewable via the public view of records.
2. Screen prints of CHRI/CJIS information or a DELJIS screen image is permitted to be sent via electronic documents/email, but must be deleted after its purpose is served, and MUST be sent through the State Secure Email (encrypted). This can also only be sent to an approved recipient as described in section E of this policy.

H. Dissemination Logging: Logging is always required and the following must be included:

1. The name of the person and agency receiving the information.
2. The date of the dissemination.
3. What was disseminated and purpose of inquiry.
4. Who disseminated the information?
5. Victim or subject's name, DOB, and SBI#.
6. Identification if information was shared verbally only or in written form (Attachment A).
I. Violations of Dissemination Rules: Violations of the laws regarding CHRI (Chapters 85 and 86 of DE Code Title 11) are considered very serious offenses. There can be loss/suspension of logon, criminal penalties, disciplinary action, or termination.

1. A person who knowingly and wrongfully destroys or falsifies a criminal history computer record or a manual criminal history record is guilty of a Class E Felony.
2. A person that permits someone else to destroy or falsify a criminal history computer record or a manual criminal history record is guilty of a Class E Felony.
3. A person knowingly sells the record for profit is guilty of a Class E Felony.
4. A person that gives CHRI to a person or agency not authorized to receive it is guilty of a Class A Misdemeanor.
5. Authorized Users who become aware of improper access of CJIS by another user, or by any other entity, shall report the violation to their Supervisor or directly to DELJIS immediately.

<table>
<thead>
<tr>
<th>Review Date:</th>
<th>Reviewed By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/1/14</td>
<td>Nancy L. Duty</td>
</tr>
</tbody>
</table>