

***Policy Name***: Use and Security of Criminal Justice Information

***Policy #:*** 01.08.03 ***Effective Date:*** December 4, 2023

***Repeals:*** None

***References:*** DYS Information Security Policy

DYS Background Check Process for New and Current Employees

 101 CMR 15.00 and 28 CFR 20

 FBI CJIS Security Policy

 G.L. c. 18A, § 10

 Public Law 92-544

 G.L. c. 6, § 172

***Signature:***   ***12/04/2023***

Cecely A. Reardon, Acting Commissioner

***Applicability:*** This policy shall apply to DYS employees, interns, volunteers, contractors, or any other individual with access to CJIS electronic or physical media and applies to equipment that processes, stores, and/or transmits CJI.

**Policy**

It is the policy of the Department of Youth Services (DYS or “the Department”) to comply with the state federal requirements for accessing the data necessary to complete state and national criminal background checks for its employees as well as obtain information to effectively supervise and support DYS youth. DYS operates fixed and mobile Criminal Justice Information System (CJIS) CJIS Terminals and handles and disposes of Criminal Justice Information (CJI) included but not limited to Criminal Offender Record information (CORI) and Criminal History Record Information (CHRI) generated from or maintained within CJIS consistent with these requirements.

DYS locates CJIS Terminals in secure DYS locations and only DYS employees with authorization to access CJIS are allowed entry into these locations. Access to CJIS is for criminal justice purposes only and no individual shall access CJIS for any purposes other than those allowed under this policy and procedures or any other applicable statutes, regulations, policies, and procedures. DYS shall not modify or alter CJIS Terminals or any other CJIS equipment from their original configuration without proper authorization from the Department of Criminal Justice Information System (DCJIS). Damage to any CJIS Terminals or unauthorized access shall be immediately reported to a supervisor, through the DYS Serious Incident Reporting Policy, and to DCJIS.

Persons found non-compliant with state or federal laws, the current FBI CJIS Security Policy, DCJIS policies or regulations, or other applicable rules or regulations, including the DYS/Executive Office of Health and Human Services’ Information Security Policy, will be formally disciplined. Discipline can include, but may not be limited to, counseling, the reassignment of CHRI responsibilities, dismissal, civil penalties, or prosecution. DYS’ employee discipline is in the discretion of DYS and will be based on the severity of the infraction, any applicable collective bargaining agreement, civil service rules or contractual agreements covering third party workforce. In addition to any discipline imposed by the Department, a CJIS user may be subject to federal and state civil and criminal penalties for improper access or dissemination, or information obtained from or through CJIS pursuant to G.L. c. 6 sec., 167A(d), 168 and 178 and 28 CFR 20.

In accordance with its commitment to the security of confidential information, including but not limited to CJI, DYS has promulgated an Information Security Breach policy to address any information security breach.

**Procedure**

A. Definitions

1. The following definitions shall have the meanings assigned to them in this policy for purposes of interpreting this policy.

Communication Information Center (CIC): DYS Central Office Unit staffed twenty-four hours per day, seven days per week with responsibilities that include but are not limited to, receiving reports of serious incidents, coordinating the issuance of warrants, making notifications to Executive leadership and senior managers, and performing other emergency related tasks.

Criminal Justice Information (CJI): Any information about an individual, available from the Criminal Justice Information System. Said information includes, but is not limited to state and interstate criminal history and Juvenile record information, protective orders, missing and wanted person files, drivers’ license and motor vehicle information, firearms licensing and gun sales transactions and other critical criminal justice information via the Board of Probation (BOP), Criminal Offender Record Information (CORI), the FBI’s National Crime Information Center (NCIC) and the Interstate Identification Index (III), the International Justice and Public Safety Network (Nlets), the Massachusetts Warrant Management System, and the Automated Licensing and Registration System (ALARS) maintained by the Registry of Motor Vehicles.

Criminal Justice Information Systems (CJIS): The computerized network, services and applications that allow state and national law enforcement and criminal justice agencies secure access 24 hours per day 7 days a week to state and interstate criminal history and Juvenile record information, protective orders, missing and wanted person files, drivers’ license and motor vehicle information, firearms licensing and gun sales transactions and other critical criminal justice information via the Board of Probation (BOP), Criminal Offender Record Information (CORI), the FBI’s National Crime Information Center (NCIC) and the Interstate Identification Index (III), the International Justice and Public Safety Network (Nlets), the Massachusetts Warrant Management System, and the Automated Licensing and Registration System (ALARS) maintained by the Registry of Motor Vehicles.

CJIS Terminals: Agency computer equipment that is authorized to have hardware and/or software containing or allowing access to CJIS and/or connect to the CJIS. Such CJIS Terminals are available through the DYS Central Office Communication Information Center (CIC) and Human Resources Units.

Department of Criminal Justice Information System (DCJIS): The Agency for the Commonwealth of Massachusetts that has responsibilities to the FBI CJIS Division that include ensuring user agencies are provided with 24-hour access to national criminal justice information, ensuring quality control for all data entered into the NCIC systems, managing policy compliance for all CJIS/NCIC users, and providing training and testing in the use of NCIC systems.

DYS Youth: Detained, committed or YES youth under care and/or custody of DYS.

Electronic Media: Information kept on memory devices, laptops, computers, and any other removable, transportable digital memory media such as a flash drive or memory card.

Executive Office of Technology Supports and Security (“EOTSS”): The Massachusetts agency responsible for establishing connectivity to the CJIS environment.

Physical Media: Information that includes printed documents and imagery that contains CJI.

Statewide Applicant Fingerprint Identification Services-Results User (SAFIS-R): The designated individuals who will be the recipients of the fingerprint based criminal record check results.

1. Terms that are defined in Policy #01.01.04, “Policy Definitions,” shall have the meanings assigned to them in that policy, unless a contrary meaning is specified in the policy.
2. Terms not defined in Policy #01.01.04 or in this policy shall have the meanings assigned to them by reasonably accepted standard dictionary definitions of American English.

B. CJIS Terminals

1. The DYS Communication Information Center (CIC) shall maintain a list of each CJIS Terminal location and a list of individuals with authorized access to the CJIS Terminals. The list must be reviewed by the Commissioner, or designee, every 6 months and is subject to review by DCJIS at any time.

2. Authorized uses of CJIS Terminals by authorized DYS personnel include:

* 1. Criminal juvenile justice duties related to the supervision of DYS Youth, including warrant entry, review of juvenile and criminal records, CJI and investigation of youth.
	2. Background check investigations of DYS employees, certain contracted providers, contractors, placement resources, interns, and/or volunteers as related to their current or prospective involvement with DYS and/or access to DYS Youth.
1. Unauthorized use of CJIS Terminals is strictly prohibited and is punishable by a fine, suspension and/or incarceration. Unauthorized uses include, but are not limited to:
	1. Use for non-criminal purposes.
	2. Private transactions.
	3. Modification/altering CJIS equipment without authorization from DCJIS; or
	4. Sharing CJI with any person or agency not authorized to receive it.
2. All authorized CJIS Terminals shall be in a secure location that includes:

a. An area, room or rooms with physical and personnel security controls sufficient to protect the CJIS Terminal that is separated from non-secure locations and has prominent posted signage denoting that it is a secured area.

b. A door or physical access point that can be secured to prevent unauthorized individuals access and be locked when unattended; and

c. The ability to position a CJIS Terminal so as to prevent unauthorized individuals from viewing or accessing any information.

1. Unless otherwise authorized, the DYS Background Check Specialist office and CIC are the designated areas for the day-to-day access and storage of CJI.
2. Unauthorized individuals shall not be allowed access to the secured CJIS Terminal locations. If there is a need for unauthorized persons to the designated areas where CJI is maintained or processed (at rest or in transit), they will be escorted by, or be under the supervision of, authorized personnel at all times. Unauthorized access shall be reported pursuant to the DYS Information Security Policy, the DYS Serious Incident Policy and the applicable policies of DCJIS and the Executive Office of Technology Services and Security Office of Technology and Information Service (EOTSS).
3. Any damage to a CJIS Terminal or unauthorized access found by DYS shall be immediately reported through the Information Security Policy, Serious Incident Policy and to DCJIS and the MA Office of Technology and Information Service (OTIS).
4. Only those DYS officials and employees who require CJIS Terminal access for their official duties as determined by the Commissioner shall have access. Individuals who may require CJIS Terminal access as a part of their official duties include but are not limited to: Human Resource employees or liaisons responsible for hiring, submitting CJI authorization requests and processing job applications and employees of CIC.
5. Prior to obtaining access to a CJIS Terminal, an employee must:
6. Have a fingerprint based criminal record check prior to hire and at least once every two years thereafter. No individual with a felony conviction is allowed access to the CJIS Terminal. DYS may request a waiver for access through DCJIS for an individual with a misdemeanor conviction. In addition, an individual believed to be a fugitive from justice, or having an arrest history without convictions, will be reviewed to determine if access to CJI is appropriate. The DCJIS will take into consideration extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

b. Be trained, tested, and certified regarding CJI and Security Awareness Training before using a CJIS Terminal or having access to CJI.

c. Receive biannual recertification regarding CJI and Security Awareness.

d. If required for their regular duties, log on to the network once at the beginning of the workday using only their assigned password and not share this password with any other user. Such users shall log off at the end of the workday; and

e. Protect and control electronic and physical access to CJI while at rest and in transit and not allow any unauthorized access to CJIS Terminal under their password.

1. Access to the CJIS Terminal by an authorized individual will be suspended if such individual is subsequently arrested and/or convicted of a crime until the outcome of the arrest is determined and reviewed by the DCJIS in order to determine if continued access is appropriate. Such access will be suspended indefinitely if a conviction results in a felony of any kind. Further, such access may be denied by the DCJIS where it is determined that access to CJI by the individual would not be in the public’s best interest.
2. DYS CIC shall monitor the CIC CJIS Terminals and printers 24 hours a day, 7 days a week, fifty-two weeks a year to respond to hit confirmations on DYS youth as well as receive reports of serious incidents, coordinate the issuance of warrants and perform emergency related tasks.

C. Access to CJI

 1. Only those DYS officials and employees who require CJI for their official duties as determined by the Commissioner shall have CJI access. Individuals who may require CJI access as a part of their official duties include but are not limited to: Human Resource employees or liaisons responsible for hiring, submitting CJI authorization requests and processing job applications, case workers and District Managers and Detention Coordinators.

2. Any DYS employee requiring CJI as a part of their job duties shall be required to complete the following prior to CJI access:

a. a fingerprint-based background check

b. a review of the educational and relevant training materials regarding CJI laws and regulations made available by DYS and DCJIS.

D. Verifying Identity of CJI

1. CIC CJIS operators shall compare and verbally verify the identity of DYS youth when CJI information is needed and only share information as required for the DYS employee’s duties associated with the youth.

2. When conducting background checks on DYS employees, certain contracted providers, contractors, placement candidates, interns, and/or volunteers as related to their current or prospective involvement, the DYS Background Check Specialist shall closely compare the CJI with the signed CORI Acknowledgement Form to determine if the CJI belongs to that individual.

3. The DYS Background Check Specialist shall provide the background check subject with a copy of the CJI and the source of the CJI prior to inquiring from the individual about such information.

E. Determining Suitability of Hiring and Notification of Decisions

1. If CJI is identified to belong to a background check subject, DYS shall follow the DYS Background Check Procedures attached to this Policy regarding decisions on hiring, notifying the individual of the CJI and the process for disputing the CJI and/or seeking a waiver in accordance with 101 CMR 15.

F. Secondary Dissemination of CJI

Any secondary dissemination of CJI must be recorded in the Secondary Dissemination log. The Secondary Dissemination log is subject to audit by the DCJIS and the FBI. The Secondary Dissemination log shall be maintained by CIC and include:

1. CJI Subject Name.
2. CJI Subject Date of Birth.
3. Name of the individual to whom the information was disseminated.
4. The entity or agency for which the requestor works.
5. Contact information for the requestor; and
6. The specific reason for the request.

G. Protection of CJI

1. All individuals with authorized access to physical or electronic media that contains CJI shall keep it protected and securely stored within physically secured locations or controlled areas. Access to such media is restricted to authorized personnel only and shall be secured when not in use or under the supervision of an authorized individual.

2. CIC or any other CJIS operator shall not disseminate CJI information to users not authorized to receive CJI.

3*.* Physical CJI shall be maintained within a lockable filling cabinet, drawer, closet, office, safe, vault, or other secure container.

4. Electronic CJI media is secured through encryption as specified in the FBI CJIS Security Policy and includes, but is not limited to discs, CDs, SDs, thumb drives, DVDs, that can be maintained within a lockable filling cabinet, drawer, closet, office, safe, or vault, or other secure container.

5. Should the need arise to move any form of CJI media, including physical CJI media (paper/hard copies) and electronic CJI media (e.g., laptops, computer hard drives, or any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card), outside of the secured location or controlled area, the transport of the CJI media will be conducted by authorized personnel ***only***. Authorized personnel will take every precaution to protect electronic and physical CJI media while in transport, and/or prevent inadvertent or inappropriate disclosure and use. Authorized personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled or secured location.
2. Restrict the pick-up, receipt, transfer, and delivery to authorized personnel.
3. Secure hand carried, electronic and paper CJI by:
	1. Storing the documents, or the electronic media containing the document, in a closed bag, briefcase, or folder.
	2. Viewing or accessing the CJI only in a physically secure location.
	3. Packaging hard copy printouts in such a way as to not have any CJI viewable.
	4. Mailing or shipping CJI only to authorized individuals (including the individual who is the subject of the CJI and only by either U.S. Mail or by another shipping method that provides for complete shipment tracking and history. The package should not be marked as confidential.

H. Disposal of Physical Media

1. Once physical CJI media (paper/hard copies) is determined to be no longer needed by the agency, it shall be destroyed and disposed of appropriately.

2. DYS will ensure physical CJI media is destroyed by shredding, crosscut shredding, or incineration by authorized personnel as follows:

1. The DYS HR Unit authorized personnel shall witness or conduct the disposal.
2. The physical media shall be shredded three (3) years after the record was generated.

I. Storage of CJI

1. DYS shall only store CJI for extended periods of time when needed for the integrity and/or utility of an individual’s personnel file and/or for research purposes.

2. DYS in conjunction with EHS IT shall implement administrative, technical, and physical safeguards, which follow the most recent FBI CJIS Security Policy, to ensure the security and confidentiality of CJI. Each individual involved in the handling of CJI shall be familiar with these safeguards.

3. Each individual involved in the handling of CJI will strictly adhere to the policy on the storage and destruction of CJI.

J. Retention of CJI

1. Once the CJI of an individual is received, it will be securely retained in internal DYS documents for the following purposes ***only***:

a. Historical reference and/or comparison with future CJI requests.

b. Disputing the accuracy of the record.

2. CJI will be kept for the above purposes in hard copy form in a locked file located in the locked office of the DYS Background Check Coordinator

K. Local Agency Security Officer (LASO)

1. DYS has designated a Local Agency Security Officer. Such individual:

a. Is considered part of the National Criminal Justice Association’s (NCJA) ‘authorized personnel’ group.

b. Completes a fingerprint check for appropriate access to CJI.

c. Identifies who uses/accesses CJI and/or systems with access to CJI

d. Identifies and documents any equipment connected to the state system

e. Ensures personnel security screening procedures are followed pursuant to policy

f. Ensures approved and appropriate security measures are in place and working

g. Supports policy compliance and ensures DCJIS Information Security Officer (ISO) is promptly informed of security incidents.

2. When changes in the LASO appointment occur, DYS shall complete and return a new LASO appointment form to DCJIS (I’m guessing) and maintain the most current copy of the form.

3. Personnel Termination:The LASO or DYS Human Resource Liaison (who is an authorized user) shall complete a Personnel Employment Termination (PET) form for any terminated authorized user. LASO shall terminate access to CJI within 24 hours of receiving notification of authorized user’s termination. The LASO shall also:

a. Arrange for the immediate return of access cards and keys to the building/offices, including but not limited to keys to the rooms and files where CJI is stored, and any files containing CJI.

b. Notify the DYS and EOHHS systems administrators to disable the terminated staff’s access to the DYS Background Check System, e-mail and VG accounts.

c. Notify DCJIS of the termination of any individual authorized to access CJI who is also a SAFIS-R User. This notification shall be made immediately upon the termination of the user and shall be accomplished by emailing a SAFIS-R User Designation Form with the “Remove” checkbox checked to the DCJIS SAFIS Unit at safis@state.ma.us.

4. Personnel Transfer:

1. LASO shall, within 24 hours of notice of transfer, review the job duties of any individual with access to CJI who has been reassigned or transferred to ensure access is still appropriate. If continued access is determined to be inappropriate, the LASO shall immediately:

a. disconnect access to CJIS.

b*.* arranges for the individual to return any access cards and/or keys to the building/office, rooms and file cabinets where CJI is kept; and

*c.* disable email, VG accounts and access to the DYS Background Check System

d*.* notifies the DCJIS of the transfer of any individual authorized to access CJI who is also a SAFIS-R User and for whom it is determined that CJI access is no longer appropriate. This notification shall be made immediately upon the termination of the user and shall be accomplished by emailing a SAFIS-R User Designation Form with the “Remove” checkbox checked to the DCJIS SAFIS Unit at safis@state.ma.us.

L. Incident Response

1. Each employee shall immediately report potential or actual security incidents to minimize any breach of security or loss of information, including CJI as follows:

a. The DYS Information Security Policy, #01.08.02 requires an employee to immediately report relevant information about an actual or potential security incident or breach to the DYS Location Manager. The Location Manager shall immediately, as soon as practical after discovery of the breach, report to DYS General Counsel and where CJI is implicated, the LASO, and complete a DYS Serious Incident Report and Information Security Incident Report.

b. Executive Office of Health and Human Services (“EOHHS”) Data Protection Policy and Procedures requires an employee to immediately report any incident involving the known or suspected privacy incident to the Systems Support Desk at systemssupporthelpdesk@massmail.state.ma.us or 617-367-5500 and to the EOHHS Chief Privacy Officer at privacy.officer@state.ma.us. A privacy incident is defined as the acquisition of PII by an unauthorized person or entity, the disclosure of personally identifiable information (‘PII”) to an unauthorized person or entity, or the access to or use of PII by and unauthorized person or entity or for an unauthorized purpose.

2. Every information security breach incident will be documented and tracked in JJEMS and the Information Security Breach Incident Log which is maintained by the DYS General Counsel’s Office.

3. The DYS General Counsel and LASO will review the information security breach incident involving CJI and implement disclosure procedures set forth in G.L. c. 93H, if required.

4. In addition to the above, LASO shall report all CJI security-related incidents to the DCJIS ISO within 48 hours. The LASO shall complete an NCJA Security Incident Report Form and shall email it to the DCJIS ISO at safis@state.ma.us.

M. Penalties for Improper Access, Dissemination and Handling of CJI

1. An employee who improperly accesses or disseminates CJI will be subject to disciplinary action up to and including, loss of access privileges, civil and criminal prosecution and termination.

2. In addition to any discipline imposed by the Department of Youth Services, a CJIS user may be subject to federal and state civil and criminal penalties for improper access or dissemination, or information obtained from or through CJIS pursuant to G.L. c. 6 sec., 167A(d), 168 and 178 and 28 CFR 20.