


<b>MELROSE POLICE DEPARTMENT</b>		Department Manual: Policy No. 4.07
Subject: <b>USE OF C.J.I.S. &amp; C.O.R.I.</b>		
• MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: N/A		<b>GENERAL ORDER</b> <b>19-005</b>
Issued: 1/17/2010 Revised: 10/15/2019	Issuing Authority <i>Michael L. Lyle</i> Michael L. Lyle Chief of Police	

## I. GENERAL CONSIDERATIONS AND GUIDELINES

The purpose of this policy is to establish guidelines for the proper operation of fixed, mobile, and portable criminal justice information system (CJIS) workstations, and to ensure the lawful handling and disposal of Criminal Offender Record Information (CORI) information generated from or maintained within the CJIS network

## II. POLICY

It is the policy of the department that:

### CJIS SYSTEM ACCESS:

- A. The Department shall keep/maintain direct terminal access to the Criminal Justice Information System (CJIS).
- B. The use of a CJIS workstation is for criminal justice purposes only. These include the commission of official criminal justice duties (i.e. investigations, bookings, warrant entry etc.), qualifying an individual

for employment within a criminal justice agency, and qualifying an individual to determine his/her eligibility to possess a firearms license. It cannot be used for non-criminal purposes including transactions conducted for public and private educational establishments, municipal agencies, town government officials, etc. is strictly prohibited and is punishable by a fine, suspension of services and/or incarceration.

- C. Each operator shall immediately report any damage to a CJIS workstation to one's supervisor. It is this agency's responsibility to report an inoperable CJIS workstation to one's supervisor.
- D. No CJIS equipment including CJIS workstations, mobile data workstations or personal digital assistant/palm pilots shall be modified or altered in any way from its set up configuration, unless it is done by the DCJIS or the device's contract vendor, and then only with notification to, and concurrence of, the DCJIS.
- E. Only authorized personnel will be allowed remote access to department workstations and only authorized connections with proper access logging will be use.
- F. Any and all CJIS information passing through a network segment will be protected pursuant to FBI CJIS Security Policy.

CJIS SYSTEM ACCESS:

- A. All operators of CJIS workstations shall be trained, tested, and certified under procedures set forth by the DCJIS before using a workstation and shall be re-certified biannually thereafter.
- B. Each CJIS workstation operator shall use one's assigned password when accessing the CJIS network and shall not give this password to anyone under any circumstances. No one shall use the network under another individual's password.
- C. All operators shall log on to the network at the beginning of one's work day and shall log off at the end of one's work day to ensure that transactions are logged under the appropriate user name. This will prevent one operator from being held responsible for another operator's CJIS transactions. Appropriate care will be taken to not allow any unauthorized access to CJIS.
- D. Agencies entering records into CJIS must monitor their CJIS workstation(s) and printer(s) twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year, to perform hit confirmations.

- E. A. Authorized personnel shall protect and control electronic and physical access to CJI while at rest and in transit.
- F. The Department has implemented appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use must be reported to the on-duty supervisor.
- G. All personnel must follow the established procedures for securely handling, transporting, and storing media.
- H. When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store, and/or transmit CJI and classified and sensitive data shall be properly disposed of in accordance with the measures described herein

FINGERPRINT REQUIREMENTS:

- A. The CJIS User Agreement and the FBI CJIS Security Policy require each CJIS agency to conduct fingerprint-based criminal record checks on all personnel prior to hire and at least once every two years thereafter. In addition, agencies must conduct fingerprint-based criminal record checks on all other individuals who have unescorted access to secure (non-public) areas of the agency prior to allowing access. These individuals include city/town IT personnel, contractors, vendors, custodians, and volunteers.
- B. These background check requests are submitted either as criminal justice employment checks (for all employees of the department) or as criminal justice checks (all non-employees) and can be done on your live-scan fingerprinting device. There is no fee for these checks.
- C. Important: with regard to fingerprint-based background checks conducted on non-department personnel, no information received in response to a fingerprint-based check may be disseminated to the individual's actual employer.
- D. If a felony conviction of any kind exists, an employee is not to be allowed access to the CJIS or to any information derived from the CJIS, and the Department is required to notify the DCJIS, in writing, as soon as practical. In the case of a non-employee, the agency must deny unescorted access to the individual.

- E. If a misdemeanor conviction exists, the Department must notify the DCJIS and must request a waiver before the employee is allowed to access the CJIS or CJI, or before the non-employee is provided unescorted access to secure areas.
- F. A part of their respective auditing programs, both the DCJIS and the FBI will check to ensure that the appropriate fingerprint-based background checks have been completed by the agency being audited. An agency which has not conducted these fingerprint-based checks as required will be found out-of-compliance in this area.
- G. Should there be any questions about these fingerprinting requirements, contact the CJIS Support Services Unit by phone at 617.660.4710 or via email at [cjis.support@state.ma.us](mailto:cjis.support@state.ma.us).

### III. SCOPE

- A. The scope of this policy applies to any electronic or physical media containing CJI while being stored, accessed, or physically moved from the Department. This policy also applies to any authorized person who accesses, stores, and/or transports electronic or physical media containing CJI. Transporting CJI outside of the Department must be monitored and controlled.

### IV. DEFINITIONS

**Electronic media**- includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

**Physical media**-includes printed documents and imagery that contains CJI

### V. PROCEDURE FOR THE USE OF CJIS

Each CJIS workstation and the information obtained from it are to be handled in conformity to the policies and guidelines set forth by:

1. The Massachusetts General Laws
2. The Code of Massachusetts Regulations (CMR)
3. 28 code of Federal Regulations 20.

4. The Massachusetts Department of Criminal Justice Information Services through manuals, training, CJIS Administrative Messages, information contained on the CJIS Extranet, and information disseminated at the Regional Working Groups meetings.

## **A. CORI OVERVIEW**

- A. The Massachusetts Public Records Law (G.L. c. 4, § 7) gives the public the right of access to most records maintained by a government agency. However, CORI information, including that which is obtained from the CJIS network is exempt from public access under the CORI Law (G.L. c. 6, §§ 167-178).
- B. CORI is data compiled by a criminal justice agency concerning an identifiable individual and which relates to the nature of an arrest, criminal charge, judicial proceeding, incarceration, rehabilitation or release, and may include a juvenile tried as an adult.
- C. Under 803 CMR, only those officials and employees of criminal justice agencies, as determined by the administrative heads of such agencies, shall have access to CORI. Criminal justice employees are eligible to receive CORI as needed during the course of their official duties.
- D. Reasons for conducting a board of probation (BOP) check may include, but is not limited to:
  - I. an investigation
  - II. an arrest
  - III. an individual applying for criminal justice employment
  - IV. local licensing purposes (i.e. where the police department is the licensing agency) and door-to-door sales people where the municipality requires the police department to regulate, and
  - V. Firearms licensing purposes.
- E. The officer may share CORI with other officers or criminal justice agencies when an investigation is being conducted, however, the dissemination must be logged in the agency's secondary dissemination log with the date, time, individual checked, purpose, officer's name, and the agency and agent to whom the information

was given.

- F. A local municipal agency seeking CORI must apply to the DCJIS for CORI certification. If certified by the DCJIS, that agency shall submit all requests for CORI to the DCJIS.
- G. Anyone requesting a copy of his or her own CORI shall be given a form to request such information from the DCJIS, or be directed to the DCJIS Web site, [www.mass.gov/cjis](http://www.mass.gov/cjis), to print the form.
- H. Many non-criminal justice agencies have been authorized by the DCJIS to receive CORI information under G.L. c. 172 (a). Such authorization was given to these agencies in writing, and a copy of this letter should be provided by these requesting agencies to the agency or police department that will be providing the requested CORI information.
- I. All other requests for CORI shall be referred to the Chief's office.
- J. To lawfully obtain CORI and to then furnish the information to any person or agency not authorized to receive is unlawful and may result in criminal and/or civil penalties (G.L. c. 6, § 177 and § 178).
- K. All complaints of CORI being improperly accessed or disseminated shall be handled as a citizen complaint and the Chief shall be advised of the matter. The complainant shall also be advised that they may file a complaint with the DCJIS by calling (617) 660-4760.

## **B. CORI**

- A. This policy is applicable to the criminal history screening of prospective and current employees, subcontractors, volunteers and interns, professional licensing applicants, and applicants for the rental or leasing of housing.
- B. Where Criminal Offender Record Information (CORI) and other criminal history checks may be part of a general background check for employment, volunteer work, licensing purposes, or the rental or leasing of housing, the following practices and procedures will be followed:

## **1. CONDUCTING CORI SCREENING**

- A. CORI checks will only be conducted as authorized by the DCJIS and MGL c. 6, §.172, and only after a CORI Acknowledgement Form has been completed.
- B. With the exception of screening for the rental or leasing of housing, if a new CORI check is to be made on a subject within a year of his/her signing of the CORI Acknowledgement Form, the subject shall be given seventy two (72) hours' notice that a new CORI check will be conducted.
- C. If a requestor is screening for the rental or leasing of housing, a CORI Acknowledgement Form shall be completed for each and every subsequent CORI check.

## **2. ACCESS TO CORI**

- A. All CORI obtained from the DCJIS is confidential, and access to the information must be limited to those individuals who have a "need to know". This may include, but not be limited to, hiring managers, staff submitting the CORI requests, and staff charged with processing job applications. (Requestor Organization Name) must maintain and keep a current list of each individual authorized to have access to, or view, CORI. This list must be updated every six (6) months and is subject to inspection upon request by the DCJIS at any time.

## **3. CORI TRAINING**

- A. An informed review of a criminal record requires training. Accordingly, all personnel authorized to review or access CORI at will review, and will be thoroughly familiar with, the educational and relevant training materials regarding CORI laws and regulations made available by the DCJIS.
- B. All personnel authorized to conduct criminal history background checks and/or to review CORI information will review, and will be thoroughly familiar with, the educational and relevant training materials regarding CORI laws and regulations made available by the DCJIS.

#### **4. USE OF CRIMINAL HISTORY IN BACKGROUND SCREENING**

- A. CORI used for employment purposes shall only be accessed for applicants who are otherwise qualified for the position for which they have applied.
- B. Unless otherwise provided by law, a criminal record will not automatically disqualify an applicant. Rather, determinations of suitability based on background checks will be made consistent with this policy and any applicable law or regulations.

#### **5. VERIFYING A SUBJECT'S IDENTITY**

- A. If a criminal record is received from the DCJIS, the information is to be closely compared with the information on the CORI Acknowledgement Form and any other identifying information provided by the applicant to ensure the record belongs to the applicant.
- B. If the information in the CORI record provided does not exactly match the identification information provided by the applicant, a determination is to be made by an individual authorized to make such determinations based on a comparison of the CORI record and documents provided by the applicant.

#### **6. INQUIRING ABOUT CRIMINAL HISTORY**

- A. In connection with any decision regarding employment, volunteer opportunities, housing, or professional licensing, the subject shall be provided with a copy of the criminal history record, whether obtained from the DCJIS or from any other source, prior to questioning the subject about his or her criminal history. The source(s) of the criminal history record is also to be disclosed to the subject.

#### **7. DETERMINING SUITABILITY**

- A. If a determination is made, based on the information as provided in section V of this policy, that the criminal record belongs to the subject, and the subject does not dispute the record's accuracy, , then the determination of suitability for the position or license will be made. Unless otherwise provided by law, factors considered in determining suitability may include, but not be limited to, the following:



- (a) Relevance of the record to the position sought;
- (b) The nature of the work to be performed;
- (c) Time since the conviction;
- (d) Age of the candidate at the time of the offense;
- (e) Seriousness and specific circumstances of the offense;
- (f) The number of offenses;
- (g) Whether the applicant has pending charges;
- (h) Any relevant evidence of rehabilitation or lack thereof; and
- (i) Any other relevant information, including information submitted by the candidate or requested by the organization.

The applicant is to be notified of the decision and the basis for it in a timely manner.

## **8. ADVERSE DECISIONS BASED ON CORI**

- A. If an authorized official is inclined to make an adverse decision based on the results of a criminal history background check, the applicant will be notified immediately. The subject shall be provided with a copy of the organization's CORI policy and a copy of the criminal history. The source(s) of the criminal history will also be revealed. The subject will then be provided with an opportunity to dispute the accuracy of the CORI record. Subjects shall also be provided a copy of DCJIS' ***Information Concerning the Process for Correcting a Criminal Record***.

## **9. SECONDARY DISSEMINATION LOGS**

- A. All CORI obtained from the DCJIS is confidential and can only be disseminated as authorized by law and regulation. A central secondary dissemination log shall be used to record *any* dissemination of CORI outside this organization, including dissemination at the request of the subject.

## **C. INTERSTATE IDENTIFICATION INDEX**

- A. Interstate Identification Index (III) checks may only be made for three (3) purposes: the administration of criminal justice; background check of a person applying for criminal justice employment; background check of a person applying for a Firearms Identification Card or a Firearms License to Carry Permit.

- B. Each agency must be able to identify a requestor of internal III inquires.
- C. Whenever III information is disseminated internally or externally to another criminal justice agency, it must be logged in the agency's III Records Check Log with the same information provided in the Agency's Secondary Dissemination Log.

## **1. NCIC FILES POLICY COMPLIANCE SUMMARY**

- A. This Department must ensure that caution indicators are set properly for wanted person file entries and explained in detail under the Misc. field
- B. When entering Wanted Persons and/or Missing Persons, Vehicle, and any other records into the CJIS/NCIC system, one must make certain that all records are entered in a timely manner being sure to include all available information to create a complete record.
- C. Invalid records should be removed promptly from the CJIS network to guarantee integrity of the data.
- D. Every entry made into the CJIS/NCIC system should be subject to a second party check to ensure accuracy of the record.

## **2. NATIONAL INSTANT CRIMINAL BACKGROUND CHECKS SYSTEMS SURVEY (NICS)**

- A. NICS can only be used for Firearms Licensing purposes, no other transactions are authorized. Per the FBI, 'NICS can't be used for employment screening of any type, or to check on individuals used as references for firearms related permits. Finally, the NICS cannot be used for law enforcement investigations outside the scope of the Gun Control Act in conjunction with the Alcohol Tobacco Firearms and Explosives.'

# **VI. PROCEDURES FOR THE PROTECTION OF CJI**

- A. To protect CJI, every employee, contractor, intern, and temporary worker shall:
  - 1. Securely store electronic and physical media containing CJI within a locked drawer or cabinet when away from the work area for more than 5 minutes. Employees with offices must lock their office doors.

2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove CJIS in printed form or on digital media.
4. Physically protect CJI until media end of life. End of life CJI is to be destroyed or sanitized using approved equipment, techniques, and procedures. (See Media Disposal Policy)
5. Not use personally owned devices to access, process, store, or transmit CJI unless pre-approved by the Commissioner.
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to, hotel business center computers, convention center computers, public library computers, and public kiosks.
7. Store all hardcopy CJI printouts in a secure area accessible to only those employees whose job functions require them to handle such documents.
8. Take appropriate action when in possession of CJI while not in a secure area:
  - a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
  - b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. Precautions for electronic devices like laptops, use session locks and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of a physically secure location, the data shall be immediately protected using encryption.
    - i. When CJI is at rest (i.e. stored electronically) outside the boundary of a physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers, and copiers. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, and laptops.
    - ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
9. Lock or log off his/her computer when not in the immediate vicinity of the work area to protect CJI.

## **1. MEDIA TRANSPORT:**

**A.** Only sworn employees and authorized contractors are permitted to transport CJI outside of the Department. Each employee and contractor will take every precaution to protect electronic and physical media containing CJI while in transport and/or to prevent inadvertent or inappropriate disclosure and use.

**B.** Sworn employees and authorized contractors shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.
3. Include privacy statements in electronic and paper documents.
4. Secure hand carried, confidential electronic and paper documents by:
  - a. storing the documents, or the electronic media containing the documents in a closed handbag, laptop bag, brief case, etc.
  - b. viewing or accessing the CJI only in a physically secure location.
  - c. packaging hard copy printouts in such a way as to not have any CJI information viewable.
  - d. mailing or shipping CJI only to authorized individuals; **DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL**; packages containing CJI material are to be sent either only by either U.S. Mail or by another shipping method(s) that provides for complete shipment tracking and history.
5. Do not take CJI home or when travelling unless absolutely necessary.

## **2. INADVERTENT OR INAPPROPRIATE DISCLOSURE OF CJI**

- A.** If CJI is unintentionally or improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:
1. You shall verbally notify the on-duty supervisor immediately.
  2. The supervisor will communicate the situation to the Captain. The Captain, in turn will notify the Chief and the ISO of the loss or disclosure of CJI.

3. The Captain will review the incident and will implement 93H disclosure procedures if required.
4. The ISO will review the incident and, if required, will notify the FBI CJIS Chief Information Security Officer (CISO) following established procedures.

## **VII. PROCEDURES FOR THE DISPOSAL OF CJI**

### **A. Physical media**

1. Print-outs and other physical media shall be disposed of by;
  - I. Shredding, using the shredder located in Records Office

### **B. Electronic media**

1. Hard-drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) will be properly disposed of by the Information Technology Department using one or more of the following methods:
  - I. Overwriting (at least 3 times) - an effective method of clearing data from magnetic media.
  - II. Degaussing - a method to magnetically erase data from magnetic media.
  - III. Destruction – a method whereby magnetic media is physically destroyed by crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be retrieved
2. Information Technology (IT) systems that have been used to process, store, or transmit CJI and/or sensitive and classified information shall not be released from the Department's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

3. Any employee who has any type of electronic media to be destroyed is to notify his/her supervisor. The supervisor will be responsible for contacting IT Department to arrange for proper disposal of the media.

### **PENALTIES FOR IMPROPER ACCESS, DISSEMINATION AND HANDLING OF CJIS DATA**

1. An employee who improperly accesses or disseminates CJIS data will be subject to corrective disciplinary action up to and including, loss of access privileges, civil and criminal prosecution, and termination. **See Disciplinary Procedure Policy.**
2. In addition to any penalty imposed by this department, a CJIS user may be subject to federal and state civil and criminal penalties for improper access or dissemination of information obtained from or through CJIS pursuant to M.G.L. c. 6, §§ 167A(d), 168 and 178 and 28 CFR 20: *Criminal Justice Information Systems*.