Waltham Police Department
DCJIS
CHAPTER 13A

General Order Number: GO-01 2022
Effective Date: 2015/2016, 04/17, 04/2022
Accreditation Standard #:

PURPOSE:

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

SYSTEM USE:

a. 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.

b. Each operator shall immediately report any damage to a CJIS workstation to a supervisor. It is this agency's responsibility to report an inoperable CJIS workstation to the Office of Technology and Information Services (OTIS) as soon as possible. Workstation operators may be held responsible for damage done to a CJIS workstation.

c. 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.

d. Each agency must ensure that any and all CJIS information passing through a network segment is protected pursuant to FBI CJIS Security Policy.

SECURITY:

Massachusetts criminal justice agencies are reminded that any security incidents involving access, or potential access, to department systems or network, or to criminal justice information of any

kind, must be reported within forty-eight (48) hours to the Department of Criminal Justice Information Services (DCJIS), regardless of whether or not the incident involved the CJIS network or CJIS systems. This requirement is contained within the CJIS User Agreement, which is signed by the Department Agency Head, CJIS Representatives, and CJIS Technical Contact. Specifically:

a. **INCIDENT REPORTING:** A security incident is violation or a potential violation of the confidentiality, integrity and/or the availability of State/FBI CJIS data. If such an incident should occur, the agency head shall submit a fax, on agency letterhead, to 617-884-4601 within forty-eight (48) hours with the following information:

1. Date and location of incident

2. Systems affected

3. Method of detection and nature of incident.

4. Description of the incident and actions taken/resolution.

5. Date and contact information for the agency.

The FBI's CJIS Security policy also has mandatory policy and reporting requirements for security breaches:

b. **POLICY AREA 3 INCIDENT RESPONSE:** The Waltham Police Department shall establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

c. **REPORTING INFORMATION SECURITY EVENTS:** The Waltham Police Department shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

DCJIS Computer Incident/Security Form shall be used to notify DCJIS of such events.

http://www.mass.gov/eopss/docs/safis/ncja-security-incident-report-form.pdf

PHYSICAL SECURITY:

Criminal Justice Information (CJI) and information system hardware, software, and media are physically protected through access control measures. The Waltham Police department is a secure building, accessible to employees only by way of code or fob. CJIS terminals are in a supervised location with limited access. The Waltham Police Department maintains a current list of personnel with authorized access and if applicable, shall issue credentials to authorized personnel.

USER ACCOUNT VALIDATION: The Chief of Police or designee are responsible to ensure that all active user accounts which allow access to the internal DCJIS network and its resources are valid. To that end, the Commissioner and/or his/her designee shall request and review a list of all active user accounts at least once every six (6) months. As part of the review, each individual associated with an active account is:

a. Currently employed by the Waltham Police Department.

b. Authorized to access the internal DCJIS network and resources.

c. Has the appropriate access level to the network, its resources, and to directories, folders, files, etc.

d. Has had a fingerprint-supported criminal background check conducted on him/her within the last five (5) years. Sworn officers will have this check conducted at the same time as their LTC renewal. Civilian employees are required to have this check conducted in accordance with the schedule set fourth by the Waltham Police Department DCJIS Coordinator.

e. In the case of those individuals with access to CJIS resources, services and data, passed both the CJIS Certification Test and the CJIS Security Test within the past two (2) years. Any user account with greater access to the network or its resources than the duties of its owner require will be adjusted appropriately within 72 hours.

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 their 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 their work day and

shall log off at the end of their work day to ensure that transactions are logged under the appropriate user's 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.

PROVISIONS:

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

a. The Massachusetts General Laws.

b. The Code of Massachusetts Regulations (CMR).

c. 28 code of Federal Regulations 20.

d. 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.

CORI:

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:

1. An investigation.

2. An arrest.

3. An individual applying for criminal justice employment.

4. Local licensing purposes (i.e.: where the police department is the licensing agency) and door to door sales people where the municipality request the police department to regulate, and 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, 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.

INTERSTATE IDENTIFICATION INDEX (III):

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.

NCIC FILES POLICY COMPLIANCE SUMMARY:

a. Each agency 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.

NATIONAL INSTANT CRIMINAL BACKGROUND CHECKS SYSTEMS SURVEY (NICS):

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, nor can it be used for firearm releases 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.'

MEDIA DISPOSAL:

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 DCJIS and/or FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures described herein.

Physical media (print-outs and other physical media) shall be disposed of by shredding, using the shredders located in Police Operations.

If there is a large number of physical media that needs to be destroyed, it may be placed in one or more of the locked shredding bins located throughout the agency. The materials in these bins will be shred on-site by a professional shredding company contracted with the Waltham Police Department. Shredding will be supervised by the DCJIS police liaison designated by the Commanding Officer of the Community Services Division.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) will be properly disposed of by the Office of Technology and Information Services (OTIS) using one or more of the following methods:

a. **OVERWRITING (AT LEAST 3 TIMES):** An effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

b. **DEGAUSSING:** A method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

c. **DESTRUCTION:** A method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit CJI and/or classified information shall not be released from DCJIS control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

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

Any employee found to have violated this policy may be subject to disciplinary action, up to, and including termination.