MALDEN POLICE DEPARTMENT
CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS) POLICY

Massachusetts police accreditation standards referenced: 81.2.9		**GENERAL ORDER** --- **POLICY NUMBER: 013**
Effective Date: **06/22/2022** Revised Date: **Total Pages: 17**	*ISSUING AUTHORITY* Police Commissioner Salvatore Butch Gennetti ***Salvatore "Butch" Gennetti***	

I. PURPOSE

The Malden Police Department participates in and has access to local, state, and federal criminal justice information systems subject to state and federal laws regarding personnel training, distribution, and disposal of information. **81.2.9** 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) generated from or maintained within the CJIS network.

II. SCOPE

This policy applies to all employees, contractors, temporary staff, and other workers with access to CJIS and FBI systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits Criminal Justice Information (CJI) and classified and sensitive data that is owned or leased by the DCJIS. 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.

III. SYSTEM USE

The department shall keep/maintain direct terminal access to the Criminal Justice Information System (CJIS).

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. These types of transactions are strictly prohibited and are punishable by a fine, suspension of services and/or incarceration.

Each operator shall take care to ensure that no damage is done to a CJIS terminal. Care will be taken not to consume food or beverages near any terminal. Each operator shall immediately report any damage to a CJIS workstation to their respective supervisor and the department CJIS representative. It is the department's responsibility to report any inoperable CJIS equipment to the CJIS Support Services Unit of the Department of Criminal Justice Information Services (DCJIS) as soon as possible. Terminal operators may be held responsible for damage done to a CJIS workstation.

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.

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

Only authorized personnel will be allowed remote access to department workstations and only authorized connections with proper access logging will be used.

IV. SYSTEM ACCESS

All operators of CJIS workstations shall be trained, tested, and certified under procedures set forth by the DCJIS before using a workstation and within six months of employment. All users shall be re-trained, re-tested, and re-certified biannually thereafter. New employees will receive training during their orientation period that will include instruction on: use of the CJIS system, policies & procedures, system security, and CORI related issues. All employees having access to CJIS/NCIC information or systems shall be subject to thorough background and state/national criminal record checks supported by fingerprints within 30 days of employment. All CJIS operators shall be fingerprinted every 5 years. Employees who have unescorted access to secure (non-public) areas within police headquarters (IT personnel, custodial staff, support staff) shall

be subject to fingerprint-based criminal record checks and shall complete CJIS security awareness training upon hiring. All other individuals with access to secure areas (vendors, contractors, etc.) shall be escorted in these areas.

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 shall be done on the live-scan fingerprinting device. No fee will be collected for these checks.

In 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.

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. Notification will be made as soon as practical to the DCJIS. In the case of a non-employee, unescorted access will be denied.

If a misdemeanor conviction exists, notification will be made to the DCJIS and a waiver will be requested before the employee is allowed access to the CJIS or CJI, or before the non-employee is provided unescorted access to secure areas.

As 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. Failure to have completed the required fingerprint-based checks will result in the department being found out-of-compliance in this area.

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.

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.

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. Dispatchers shall monitor the CJIS Messenger program on the radio room terminal for teletypes, hit confirmations, locate notifications, error messages and any other message that may require immediate action. Any teletypes from CJIS support services that do not require immediate action shall be forwarded to the department CJIS representative.

Authorized personnel shall protect and control electronic and physical access to CJI while at rest and in transit.

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. All personnel must follow the established procedures for securely handling, transporting, and storing media.

When no longer usable, hard drives, diskettes, tape cartridges, CD's, ribbons, hard copies, printouts, 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.

V. 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

VI. PROCEDURES FOR THE USE OF CJIS

PROCEDURE

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

- The Massachusetts General Laws;
- The Code of Massachusetts Regulations (CMR);
- 28 Code of Federal Regulations 20;
- The 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 Group meetings.

CORI OVERVIEW

The Massachusetts Public Records Law (G.L. c. 4, s 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, ss 167-178).

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.

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.

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 requires the police department to regulate; and
5. firearms licensing purposes.

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.

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.

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 website, http://www.mass.gov/cjis, to print the form.

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.

All other requests for CORI shall be referred to the Office of the Chief of Police.

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, s 177 and s 178).

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.

CORI

This policy is applicable to the criminal history screening of prospective and current employees, subcontractors, volunteers and interns, and professional licensing applicants.

Where Criminal Offender Record Information (CORI) and other criminal history checks may be part of a general background check for employment, volunteer work, or licensing purposes, the following practices and procedures will be followed:

Conducting CORI Screening:

- CORI checks will only be conducted as authorized by the DCJIS and MGL c. 6 s. 172, and only after a CORI acknowledgement form has been completed.

- If a new CORI check is to be made on a subject within a year of his/her signing of the CORI acknowledgment for, the subject shall be given seventy-two (72) hours' notice that new CORI check will be conducted.

Access to CORI

- 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. The Malden Police Department will maintain and keep a current list of each individual authorized to have access to, or view, CORI. This list will be updated every six (6) months and is subject to inspection upon request by the DCJIS at any time.

CORI Training

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

Use of Criminal History in Background Screening

- CORI used for employment purposes shall only be accessed for applicants who are otherwise qualified for the position for which they have applied.
- 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.

Verifying a Subject's Identity

- 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.
- 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.

Inquiring About Criminal History

- In connection with any decision regarding employment, volunteer opportunities, or professional licensing, the subject shall be provided with a copy of the criminal history record, whether obtained directly from 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.

Determining Suitability

- If a determination is made 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 for license will be made. Unless otherwise provided by law, factors considered in determining suitability may include, but not be limited to, the following:

  i. Relevance of the record to the position sought;
  ii. The nature of the work to be performed;
  iii. Time since the conviction;
  iv. Age of the candidate at the time of the offense;
  v. Seriousness and specific circumstances of the offense;
  vi. The number of offenses;
  vii. Whether the applicant has pending charges;
  viii. Any relevant evidence of rehabilitation or lack thereof; and
  ix. 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.

Adverse Decisions Based on CORI

- 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*.

Secondary Dissemination Logs

- All CORI obtained from 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 the organization, including dissemination at the request of the subject.

INTERSTATE IDENTIFICATION INDEX

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 (FID) or License to Carry Firearms (LTC).

Each agency must be able to identify a requestor of internal III inquiries.

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 Second Dissemination Log.

NCIC Policy Compliance Summary:

The Malden Police Department must ensure that caution indicators are set properly for wanted person file entries and explained in detail under the MISC field.

When entering Wanted Persons and/or Missing Persons, Vehicles, 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.

Invalid records should be removed promptly from the CJIS network to guarantee integrity of the data.

Every entry made into the CJIS/NCIC system should be subject to a second party check to ensure the 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.

Procedures for the Protection of CJI

To protect CJI, every employee, contractor, intern, and temporary worker shall:

- 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.
- Restrict access to electronic and physical media to authorized individuals.
- Ensure that only authorized users remove CJIS in printed form or on digital media.
- Physically protect CJI until media end of life. End of life CJI is to be destroyed or sanitized using approved equipment, techniques, and procedures.
- Not use personally owned devices to access, process, store, or transmit CJI unless pre-approved by the Commissioner.
- Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to, hotel business computers, convention center computers, public library computers, and public kiosks.
- Store all hardcopy CJI printouts in a secure area accessible to only those employees whose job functions require them to handle such documents.
- 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 folder or envelope for hard copy printouts. 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.

    1. 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.

    2. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

- Lock or log off his/her computer when not in the immediate vicinity of the work area to protect CJI.

Media Transport

- Only sworn employees and authorized contractors are permitted to transport CJI outside 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.
- Sworn employees and authorized contractors shall:

    a. Protect and control electronic and physical media during transport outside of controlled areas.
    b. Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.
    c. Include privacy statements in electronic and paper documents.
    d. Secure hand carried, confidential electronic and paper documents by:

i. Storing the documents, or the electronic media containing the documents in a closed handbag, laptop bag, brief case, etc.
ii. Viewing or accessing the CJI only in a physically secure location.
iii. Packaging hard copy printouts in such a way as to not have any CJI information viewable.
iv. 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 by only either U.S. Mail or by another shipping method(s) that provides for complete shipment tracking and history.

e. Not take home or when travelling unless absolutely necessary.

Inadvertent or Inappropriate Disclosure of CJI

If CJI is unintentionally or improperly disclosed, lost, or reported not received, the following procedures must be immediately followed:

- Immediate verbal notification to the on-duty unit supervisor.
- The supervisor will communicate the situation to the Patrol Commander who, in turn, will notify the Chief and the ISO of the loss or disclosure of CJI.
- The Patrol Commander will review the incident and will implement 93H disclosure procedures if required.
- The ISO will review the incident and, if required, will notify the FBI CJIS Chief Information Security Officer (CISO) following established procedures.

PROCEDURES FOR THE DISPOSAL OF CJI

A. Physical Media
   a. Printouts and other physical media shall be disposed of by:
      i. Shredding, using one of the shredders located inside the police station.

B. Electronic Media
   a. Hard-drives, tape cartridges, CD's, printer ribbons, flash drives, printer and copier hard drives, etc. will be properly disposed of by the IT 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.

b. 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.

c. 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 the IT Department to arrange for proper disposal of the media.

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

A. 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.

B. 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 ss 167A(d), 168 and 178 and 28 CFR 20: *Criminal Justice Information Systems.*

PASSWORDS

All new employees who are CORI authorized and who have been trained and tested in the use of the CJIS system will change their DCJIS assigned password to one of their own choosing. The new password must meet the criteria described below. Each individual employee is responsible for maintaining the integrity of their password. As soon as the CJIS rep or backup rep is notified by the Chief's Office of an employee separation, the DCJIS will be notified to remove that employee's user ID from the system.

In keeping with the FBI CJIS Security Policy, as well as with industry best practices, access to any CJIS application requires the use of a strong password.

Strong passwords meet the following requirements:

- must contain a minimum of eight (8) characters
- must contain at least one number AND at least one of the following symbols
  ~!@#$%^&*()-_
- must be different from the last 10 passwords used
- cannot contain your user name, a proper name, or a dictionary word.

In addition, each CJIS user is required to change his/her password every 90 days, and each new password must meet the strong password requirements listed above.

The following security-related requirements have also been implemented in the CJIS environment:

1. Five (5) invalid logon attempts will result in the lockout of the user's account. The user will need to contact the Public Safety Data Center at 617-660-4620 to get his/her account unlocked and, if necessary, to get his/her password reset.

2. A user will be automatically logged out of all CJIS applications after 30 minutes of inactivity. The thirty-minute log out does not apply to permanently mounted devices in police vehicles or to CJIS workstations used specifically for dispatch functions. However, it does apply to all other devices, such as terminals in detective units and mobile devices not permanently attached to police vehicles.

These requirements will ensure the security and integrity of all CJIS and FBI systems and the information they contain.

BOP & TRIPLE-I QUERIES

No BOP's or Triple-I's will be disseminated to any outside person or agency. The only exception to this will be court personnel. Any such personnel requesting a criminal history will request such through the Malden PD Prosecutor's Office. A secondary dissemination log will be kept and maintained by the prosecutor's office for such instances. Under no circumstances will a user conduct a BOP or Triple-I inquiry on their own name or for purposes other than the administration of criminal justice, firearms licensing, or criminal justice employment.

SUICIDE RISK FILE

Following the booking of a prisoner by the OIC, the dispatcher will query the arrestee through the suicide risk file using the "SUI" message key. The resulting printout will be retained and attached to the arrest report. If the inquiry returns a "hit" the dispatcher will immediately notify the OIC.

Whenever a person in custody at the Malden Police Department attempts or threatens suicide, the dispatcher will enter said person into the CJIS system as a suicide risk using the "SUI" message key. This entry shall be made within twenty-four hours of such incident. An entry must be made for each threat or attempt. The resulting printout will be retained and attached to the report.

Each month, the department designated CJIS Rep or backup Rep will perform a validation of the records which are 60-90 days old, 14-15 months old, 26-27 months old, 38-39 months old, etc. The records to be validated include: boats, guns, license plates, missing persons, securities, vehicles, and NCIC warrants. The validation will be completed within 20 days.

VALIDATION

Record validation is one of the most important components of any data quality program. Since the users of CJIS and NCIC are the primary source of the information contained within these systems, each agency with records in the CJIS and NCIC databases is a vital contributor to the data quality process and is directly responsible for the accuracy of its records. Therefore, in an effort to assist agencies with this important and serious responsibility, the CJIS and NCIC validation programs were implemented.

CJIS and NCIC policy require that each agency with records in these systems have specific, step-by-step procedures for validating those records. In an effort to help users comply with these policies, the CJIS Support Services Unit (CSSU) has developed the following model validation procedures. Each agency is encouraged to implement these model procedures. At the very least, each agency must develop its own set of procedures which are as comprehensive as those contained in the model. The CSSU is available to assist each agency in the creation of validation procedures which are tailored to the needs of the specific agency.

VALIDATION DEFINITION

The following Validation Definition is from the NCIC Technical and Operational Update (TOU) 89-5:

Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during a CJIS or NCIC audit.

VALIDATION SCHEDULE

Each agency that enters records into the CJIS and NCIC systems is required to perform a monthly validation. The records to be validated each month are those which are 60-90 days old, 14-15 months old, 26-27 months old, 38-39 months old, etc. In other words, in April, an agency is required to validate all of its records that were entered during the month of January of the current year and all previous years.

The Validation schedule is as follows:

Validation Entries Made in:

January.....October
February.....November
March.....December
April.....January
May.....February
June.....March
July.....April
August.....May
September.....June
October.....July
November.....August
December.....September

SECOND PARTY CHECK

Per the CJIS and FBI/NCIC regulations all agencies entering records into the CJIS and NCIC are responsible for their accuracy, timeliness and completeness, therefore, it imperative that all entering agencies conduct Second Party Checks. This check allows all data being entered into both CJIS and NCIC to be checked by another individual to ensure the accuracy of the information. "This verification should include assuring that the available cross-checks (e.g., VIN/License Numbers) were made and the data in the CJIS and NCIC records matches the data in the investigative report. Agencies lacking support staff for this cross-checking should require the case officer to check the record, as he/she carries primary responsibility for seeking the fugitive or the stolen property" (NCIC 2000 Operating Manual, Introduction, Section 3.2,1)

Proper Usage and Timeliness of Second Party Checks
The CJIS and FBI/NCIC regulations contain a preferred method to ensure timeliness of a record that should be implemented by all entering agencies. The record being entered should be checked for accuracy and completeness by another individual on the same shift prior to submitting the record to CJIS or NCIC. However, if another individual on the same shift is not available it is the agency's responsibility to ensure the check is being conducted at the **beginning** of the next shift to ensure a timely entry.

Improper Usage of Second Party Checks
Per CJIS and FBI/NCIC policy, under no circumstances can a "Second Party Check" result in the same individual that entered the record also be the one to check the accuracy of the information. To provide further clarification, one individual cannot enter the record and simply query the record in the CJIS or NCIC to make certain the data is correct. This practice does not ensure the integrity, accuracy or completeness of the record. Any agency that utilizes this practice must cease immediately.

SEALED RECORDS

Criminal justice agencies now have direct access to Massachusetts sealed record data in accordance with M.G.L. c. 6, § 172 and G.L. c. 276, § 100D. Sealed records are available to criminal justice agencies as defined in G.L. c. 6, § 167 for the performance of their official criminal justice duties and as otherwise authorized by law. In addition, sealed records may include Criminal Offender Record Information (CORI) and juvenile criminal history otherwise regulated under G.L. c. 6, § 172 and G.L. c. 119, § 60A. The DCJIS has developed the following guidelines regarding proper access to, and use of, sealed record information.

Permissible use of sealed records:

(1) Firearms licensing authorities, as defined in G.L. c. 140, § 121, may access sealed records for the purpose of firearms licensing in accordance with G.L. c. 140, §§ 121 to 131P.
(2) Criminal justice agencies may access sealed record data for official criminal justice purposes.
(3) The Department of Children and Families (DCF) may access sealed records as provided in G.L. c. 6, §172B for the purpose of evaluating foster and adoptive homes.
(4) Judges, court officials and probation officials may access sealed record data for criminal matters.
(5) Judges may use sealed records in civil and probate matters in accordance with the in-camera review requirements set forth in G.L. c. 276, § 100A.
(6) Custodial authorities may access sealed record data in accordance with their official criminal justice duties.

Prohibited use of sealed records:

(1) Sealed records shall not be used for criminal justice employment (see M.G.L. c. 276, § 100A).
(2) Sealed records shall not be used for the purpose of municipal licensing as authorized under a municipal by-law or ordinance in accordance with G.L. c. 6, § 172B 1/2.
(3) Use of sealed records for personal interest or curiosity is prohibited.
(4) Access to, and use of, sealed record information unrelated to the actual performance of criminal justice agency duties is prohibited.

Penalties:

The penalties for knowingly obtaining, communicating, or seeking to communicate CORI in violation of G.L. c. 6, §§ 168 through 175, as set forth in G.L. c. 6, § 178, include up to one year in a jail or house of correction and fine of up to $5,000, with an enhanced fine of up to $50,000 in the case of a violation by an entity that is not a natural person. The penalties for knowingly obtaining, communicating, or seeking to communicate juvenile criminal history data, as set forth in G.L. c. 6, § 178, include up to one year in a jail or house of correction and fine of up to $7,500, with an enhanced fine of up to $75,000 in the case of a violation by an entity that is not a natural person.

The Commissioner of the DCJIS may issue civil or administrative sanctions in accordance with the CJIS User Agreement, 803 CMR 7.00 *et seq.,* and the FBI CJIS Security Policy. In addition, CORI violations may be referred to the Criminal Record Review Board (CRRB) and may subject the individual to civil penalties of up to $5,000 for each knowing violation.

CJIS ONLINE

All employees and vendors who are not certified in the use of the CJIS system and who are permitted unescorted access inside police facilities will be required to access CJIS Online for certification.