Criminal Justice Information System (CJIS)

WILLIAMSTOWN POLICE DEPARTMENT POLICY & PROCEDURE NO. **4.41**	EFFECTIVE DATE: 03/21/2022
	REVISION DATE: 03/21/2022
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: 74.1.3; 81.2.9	REVIEW DATE: 03/21/2023

I. POLICY

To establish guidelines for the proper operation of fixed, mobile and portable Criminal Justice Information System (CJIS) workstation, and to ensure the lawful handling and disposal of Criminal Offender Record Information (CORI) generated from or maintained within the CJIS network. CJIS is the state's criminal justice computer system. **[81.2.9]**

II. PROCEDURE

Unauthorized persons must not be allowed to view sensitive information on printouts or monitors. All printouts which contain CORI data shall be shredded when no longer needed.

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

- Massachusetts General Laws
- Code of Massachusetts Regulations (CMR)
- 28 Code of Federal Regulations 20.
- DCJIS through manuals, training, CJIS Administrative Messages, information contained on the CJIS Extranet, and information disseminated at the Regional Working Groups meetings.
- CHSB CJIS User Agreement
- FBI CJIS Security Policy

All Department members are required to comply with the policies, procedures and guidelines in the CJIS Operators Manual, the CJIS User Agreement and this Policy and Procedure.

Use of a CJIS workstation is for criminal justice purposes only.
Use of the system for non-criminal purposes is strictly prohibited and is punishable by a fine, suspension of services and/or incarceration. All inquiries or system use for non-criminal justice related purposes is strictly prohibited and may subject the department and/or the individual making the inquiry to federal and state civil and criminal penalties. **Transactions conducted for public and private educational establishments, municipal agencies, town government officials, etc. are also prohibited.**

M.G.L c.266, s.120F states that "[w]hoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both. The requirement of a password to gain access shall constitute notice that access is limited to authorized users." Even if a police officer was authorized to access the Criminal Justice Information System (CJIS) for official use in the normal course of his/her duties, after gaining access to the system, he/she would know that using it for non-law enforcement purposes is not permitted.

Passwords must be kept confidential and no one else should be allowed to observe or use passwords of another, including BOP, CJIS Web, CJIS WebRMV, IMC, etc.

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 - ~ ! @ # $ % ^ & * ( ) _

In addition, each CJIS user is required to change their password every 90 days, and each new password must meet the strong password requirements listed above. This is done automatically.

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

- Five (5) invalid logon attempts will result in the lockout of the user's account. The user will need to contact the DCJIS Support Services at 617-660-4620 to get their account unlocked and, if necessary, to get their password reset.

- 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 the booking area and mobile devices not permanently attached to police vehicles.

The Chief of Police will designate an employee to act as the Department's CJIS representative to the Criminal History Systems Board. The Chief of Police shall also appoint a backup CJIS representative and CJIS technical contact. (See CJIS User Agreement for a more detailed list of responsibilities)

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

The Chief of Police or CJIS Representative will execute a user agreement with DCJIS.

III. SYSTEM USE

- **The use of the CJIS system is for Criminal Justice purposes only.**

- Each operator shall take care to ensure that no damage is done to a CJIS accessible terminal. Care must be taken not to consume food or beverages near any computer terminal.
- Each operator shall immediately report any damage to a CJIS accessible terminal to the shift supervisor along with a follow-up email to the Department's CJIS Representative.

    - Operators may be held responsible for damage done to any computer terminal.

- Anytime a CJIS accessible terminal is inoperable the operator may call the DCJIS Support Services help line for assistance. If the terminal cannot be repaired the Department CJIS Representative shall be notified by email.

- CJIS accessible terminals shall not be modified or altered in any way from their set-up configuration, unless done by an approved member of this Department or a representative of the Department's IT staff.
- For safety reasons cruiser lap tops, or other wireless devices, shall not be used by a driver while the vehicle is in motion.
- No CJIS equipment, including CJIS workstations, mobile data 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 CHSB or the device's contract vendor, and then only with notification to, and concurrence of, the CHSB.
- Each agency must ensure that any and all CJIS information passing through a network segment is protected pursuant to FBI, CJIS Security Policy.
- Test entries during training and system checks or repairs should follow recommended formats and procedures, to avoid false "hits". The CHSB has created "test" records in the CJIS and NCIC systems which are to be used for "administrative" purposes, such as training new hires or testing new systems and applications. A list of these records is located on the CJIS Extranet web site as well. The use of any other names for testing or training purposes is prohibited.
- This policy complies with the mandates of the Criminal History Systems Board (CHSB) CJIS User Agreement.
- Registry of Motor Vehicles (RMV) inquiries may NOT be made for personal curiosity or interest. Access to, and dissemination of, information contained in the Massachusetts Registry of Motor Vehicles shall be made for official criminal justice purposes only. Improper dissemination of RMV information is a violation of federal law.

IV. SYSTEM ACCESS

The CJIS system shall only be used for criminal justice purposes. Passwords must be kept confidential and no one else should be allowed to observe or use passwords, including BOP, NexTest, CJIS Web, CJIS WebRMV, etc. Unauthorized persons must not be allowed to view sensitive information on printouts or the monitor. All printouts which contain CORI data shall be shredded when no longer needed. Violations carry potential criminal and administrative sanctions.

- Each terminal operator shall use their assigned password when accessing the CJIS network and shall not give their password to anyone

under any circumstances. No one shall access the CJIS network using another operator's password and user-name.

- All operators shall log on to the network at the beginning of their tour of duty and log off at the end of their shift to ensure that communications are logged under the appropriate user name. This will also prevent one operator being held responsible for another operator's CJIS communications.

- If an operator moves away from the immediate control of their device they shall log off from the CJIS Network.
- Appropriate care must be taken to prevent unauthorized access to CJIS.
- Agencies entering records into CJIS must monitor their CJIS workstation (s) and printer twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year, to perform hit confirmations. **[74.1.3 f]**

- A CJIS user may be subject to federal and state civil and criminal penalties for improper access and dissemination of information obtained from or through CJIS pursuant to M.G.L. c.6, 167A(d), 168 and 178 and 28 CFR 29: Criminal Justice Information Systems and is subject to department disciplinary measures.

- Access to personal information contained in motor vehicle records, including driver's license files, is governed by the Federal Driver Privacy Protection Act ("DPPA"). The DPPA makes it unlawful to access RMV data by any means, by any law enforcement official for non-official purposes. Individuals that violate the DPPA are subject to a criminal fine and may be civilly liable to the subject of the record that was improperly accessed.

- Take extra care to prevent the unauthorized use of Mobile Data Terminals, such as:
    - Assuring that unattended cars are locked, when there is a possibility of unauthorized access to the vehicle; and
    - Logging off the system, when the MDT will not be used for an extended period.
    - Log-in accounts for personnel who have been suspended, fired, retired or voluntarily terminated will be immediately disabled.

Shredding is the appropriate method for destroying CJIS and NCIC data.

Agency data processing equipment and supplies will be disposed of by shredding, incineration, or degaussing.

V. RESOURCES

The "**NCIC Code Manual**" lists the codes necessary for proper record entry. The CJIS Operating Manual contains all operations pertaining to the CJIS system. Both manuals are maintained in the Communications Center and can be found on-line under **CJIS Extranet.**

Training:

1. Each terminal operator will be trained, tested and certified as a terminal operator within six (6) months of their employment.
2. That all terminal operators are re-certified at least every two (2) years.
3. Security awareness training will be provided to all new employees within the first six (6) months of employment or reassignment, as well as, IT personnel (including vendors).
4. Security awareness training will be provided to all employees, as well as, IT personnel (including vendors) on a biennial basis.
5. The Law Enforcement Individual Agreement of Non-Disclosure will be signed by every employee every two years.
6. A CORI Vendor Agreement of Non-Disclosure will be signed by vendors before performing any work on the department CJIS systems.
7. CJIS Test Records will be used for all CJIS related training and testing.
8. The department will maintain records of all training and testing.

Only those officers whom have been certified in its use are to operate the Department's CJIS terminal.

Employment:

Pursuant to Section 5.08 of 803 C.M.R. and FBI/NCIC Policy, before employing persons whom will have access to the CJIS terminal, the Department will conduct a background check on such persons. All such persons using the CJIS terminal will have passed a pre-employment record check.

Fingerprint based background checks must be conducted prior to initial hire and at least once every five years thereafter.

This includes all:

1. Police officers
2. Regularly scheduled custodial staff, and
3. Department IT vendors with responsibility for configuring and maintaining computer systems with potential access to CJIS information.

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 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.

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.

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.

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.

VI. COMPLIANCE

CJIS and NCIC records must be entered, modified, located and cancelled in accordance with CJIS policy. Blank worksheets are under department forms.

- Department members are required to provide an original signed theft report, missing person report, or a stolen vehicle/plate/ article/ boat/ gun / part / wanted person / felony vehicle, securities and other currency, and stolen items report.
- The worksheet must be filled out with all available data and using appropriate CJIS/NCIC codes.
- Before the record is entered, a query must be made for the item, vehicle or person.
- The record must be entered into the system using data from the worksheet.
- The record must be queried again to verify the accuracy of the data.
- CJIS regulations require that all original documents and printouts must be stored in the Sergeants office. They must be placed into a folder labeled with the case number, and files in the appropriately named category.

Entry / Inquiry Requirements:

All records entered into CJIS/NCIC will contain all information available at the time of entry.

Officers will enter into CJIS/NCIC immediately all records for which the minimum entry requirements have been satisfied including the following: stolen items; motor vehicles-license plates-articles-boats-parts-guns-securities and other currency.

Officers whom seize or otherwise take into possession any of the above items will perform a stolen inquiry on each item.

All additional, relevant sources of information (such as previous arrests or R.M.V information) will be checked prior to entering any record to ensure that as complete a record as possible is entered.

For each record entry there must be:

- A signed report by the victim or reporting party.
- Initial query printouts (e.g., Q2 or QA or QG)
- "Record Not Found" response from CJIS
- "No NCIC Want" response from NCIC
- "Record Added" printout
- "Queried by GRE" printout showing a post-entry query

Second Party Check Requirement

Officers entering records into CJIS/NCIC are responsible for their accuracy, timeliness and completeness and shall conduct Second Party Checks. All data entered into CJIS/NCIC must be checked by another officer to ensure the accuracy of the information. "This verification will include assuring that the available cross-checks (i.e., VIN/License Numbers) were made and the data in the entry records matches the data in the investigative report. The case officer carries primary responsibility for seeking the fugitive or the stolen property."

Complete record

A complete record of any kind includes all information that was available on the person or property at the time of entry and any additional information that

may have been obtained upon further investigation. Validation should include a review of whether additional information which is missing from the original entry that could be added has become available for inclusion to the record.

Proper Usage and Timeliness of Second Party Checks

Records being entered must be checked for accuracy and completeness by another officer on the same shift prior to entering the records. However, if another officer on the same shift is not available, the checks must be conducted at the beginning of the next shift to ensure a timely entry.

Improper Usage of Second Party Checks

Under no circumstances can a "Second Party Check" result in the same officer that entered the record also be the one to check the accuracy of the information i.e., one office cannot enter the record and simply query the record to make certain the data is correct. This practice does not ensure the integrity, accuracy or completeness of the record.

Cancellation of Records:

Any officer upon receiving information from another agency that a wanted person has been apprehended or a missing person located, or a stolen vehicle recovered or a stolen article found, shall immediately cancel the appropriate record out of the CJIS/NCIC System. **[74.1.3 e]**

The cancellation message is to be attached to the appropriate case file/report. Said officer will up-date the applicable case file/report.

Error Notification Messages:

Messages regarding CJIS/NCIC "error notifications" will be corrected immediately by the desk officer. The record/file containing the error will be located and corrected by the desk officer.

Purged Records:

Records which have been purged from CJIS/NCIC due to the expiration of the retention period shall be reviewed by the CJIS Representative or Backup Representative, whom shall determine if such records are to be re-entered into CJIS/NCIC.

Modification to records:

Modifications to records in the CJIS/NCIC systems must be made in a timely manner and may not be left for personnel working subsequent shifts.

A timely modification of any record is one made immediately upon the receipt of additional or different information, or erroneous data.

VII. CRITICAL REMINDERS

The following subject categories should be reviewed on a regular basis. They are critical tasks which occur infrequently and may be overlooked during busy times.

Hit confirmation

Definition of a 'HIT"

A 'HIT" is a positive response from CJIS and/or NCIC in which the person or property inquired upon appears to match the person or property contained in the response.

Probable Cause

A CJIS and/or NCIC hit alone is NOT probable cause to arrest an individual or to seize property. It is one factor which must be added to other facts and circumstances to arrive at sufficient legal grounds for probable cause to arrest a person or to seize property.

However, based on the decision in U.S. v. Hensley, 83 L.Ed.2d. 604 (1985), an NCIC hit would establish reasonable suspicion to detain an individual to briefly investigate the circumstances, including verifying and confirming the CJIS and/or NCIC hit.

EXCLUSION:

A hit in the Warrant Management System (WMS) may be probable cause to arrest, provided that the arresting officer is "relying in good faith on the warrant appearing in the Warrant Management System."

Relying in good faith, an Officer can effect an arrest based solely on the entry in the Warrant Management System (WMS). If there is any doubt as to the identification of the subject, the inquiring agency should contact the agency responsible for the warrant (the WPD) and confirm the subject is identical to the subject described in the record.

RETENTION OF THE HIT RESPONSE [74.1.3 c]

1. When an operational inquiry on an individual or property yields a valid positive response (hit), the terminal-produced printout showing the inquiry message transmitted and the record (s) on file in NCIC shall be retained for use in documenting probable cause for the detention of the missing person, arrest

of the wanted person, or seizure of the property. The printout may also prove valuable in a civil suit alleging a false arrest, a false imprisonment, a civil rights violation, or an illegal seizure of property. In all cases, the original printout should be retained for use in any court proceedings.

2. When a CJIS or NCIC inquiry yields a hit, the terminal operator making the inquiry should note on the terminal-produced printout precisely how, when and to whom the information was given, initial and date this notation, and forward the printout to the inquiring officer or agency for retention in the case file. This procedure establishes the chain of evidence for the communication should the arresting officer need to substantiate actions in a judicial proceeding.

3. The printout should be retained for as long as there remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. The printout should be retained until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated.

HIT CONFIRMATION POLICY (does not include WMS warrants)

Any agency which receives a record(s) in response to a CJIS or NCIC inquiry must confirm the hit on each record(s) which appears to have been entered for the person or property inquired upon prior to taking any of the following actions: 1) arresting the wanted person; 2) detaining the missing person; 3) seizing the stolen property; 4) charging the subject with violating a protection order; or 5) denying the subject the purchase of a firearm.

Additionally, an agency detaining an individual on local charges where the individual appears identical to the subject of a wanted person record *and is within the geographical area of extradition* must confirm the hit.

Confirming a hit means to contact the agency that entered the record to [**74.1.3 d]**:

1. Ensure that the person or property inquired upon is identical to the person or property identified in the record;

2. Ensure that the warrant, missing person report, protection order, or theft report is still outstanding; and

3. Obtain a decision regarding: 1) the extradition of a wanted person when applicable, 2) information regarding the return of the missing person to the appropriate authorities, 3) information regarding the return of stolen property to its rightful owner, or 4) information regarding the terms, conditions, and service of a protection order.

Hits on records entered by this department:

If another department contacts us by a locate message, YQ message, Administrative Message, phone call or fax to inquire about a record we entered, the shift supervisor will review the original report and determine our response.

For an out-of-state department, a YR message will be transmitted to give confirmation status, in addition to any telephone conversations.

IN-STATE HIT CONFIRMATION REQUEST [74.1.3 b]

An agency seeking hit confirmation within state must contact the originating agency by TELEPHONE if possible. If unable to call, an Administrative Message must be sent.

The terminal operator making the inquiry should note on the Hard Copy printout:

1. precisely how, when and to whom the information was given;
2. the name of the person confirming the record; and
3. the time the record was confirmed.

The terminal operator should then initial and date this notation and forward the printout to the inquiring officer or agency for retention in the case file.

When using the telephone, one or more of the following should be obtained:

1. Administrative messages sent as final confirmation
2. Fax messages sent as final confirmation
3. Dispatcher audio tape recordings

Documentation of the confirmed hit is essential in that it may be critical to the success of defending a later claim of misidentification or inappropriate action.

OUT-OF-STATE HIT CONFIRMATION REQUEST [74.1.3 b]

An agency seeking an out-of-state hit confirmation must contact the entering agency via an NLETS "YQ" (Hit Confirmation Request) message. This MUST be done in addition to any telephone contacts. An agency must then respond using the hit confirmation request (YQ) message. There are two levels of priority for YQ messages: (see below)

10 Minutes (Urgent) / 1 hour (Routine)

Priority 1: Urgent

Upon receiving a hit confirmation, an officer will respond to the request within ten (10) minutes of receipt. In the event the officer cannot confirm the record within ten (10) minutes, they must indicate to the requesting agency the specific amount of time that will be needed to confirm the record.

Priority 2: Routine

All priority 2 hit confirmation requests will be responded to within one (1) hour of receipt.

An agency which receives a record in response to a NCIC inquiry must confirm the hit with the entering agency prior to taking any action based upon the record – arresting a wanted person, detaining a missing person, seizing stolen

property/vehicles/plates or charging the subject with violation of a protection order.

To confirm a hit means to contact the agency and to verify:

- That the CJIS/NCIC record is still outstanding,
- That the person or property inquired upon is identical to the person or property identified in the record,

Obtain a decision regarding: whether or not extradition will take place on a wanted person, information regarding return of a missing person to the appropriate authorities, information regarding the return of stolen property and information regarding the terms, conditions, and service of a protection order.

The department that entered the record will cancel the record when the person or property in the record is no longer considered to be wanted, missing or stolen.

Locate Messages

Every agency upon taking a person into custody, identifying a missing person, or acquiring property, after confirming the hit, must place a locate on the corresponding NCIC record(s).

The only exceptions to placing a locate message occur when the hit contains a no extradition indication or an extradition limitation indication and the agency finding the person is outside the geographical area of extradition. In such a case, the record should not be located.

Records which were entered by Massachusetts departments must be Located using the appropriate code, LA, LL, LV, LW, etc. All records which were entered by out-of-state departments must be located using the LN feature.

The procedure for sending a "locate message" is in the CJIS Operation Manual.

A hard copy of the "locate message" will be attached to the case file.

Entering warrants into NCIC and CJIS temporary warrants (See CJIS Wanted Person File) [74.1.3 a]

Agencies must have a warrant (electronic or hard copy) on file to support a wanted person entry. Only the agency that holds the warrant may make an NCIC wanted person entry.

We can enter felony warrants from WMS into the NCIC system if we want the warrant to be seen by police departments in other states.

A temporary felony want record, message key (MKE) ET, may be entered to establish a "want" entry when a law enforcement agency needs to take **prompt action** to apprehend a person (including a juvenile) who has committed, or the officer has reasonable grounds to believe has committed a **felony**.

All felony warrants for persons out-of-state in which the District Attorney authorizes extradition will be entered into CJIS/NCIC.

Out-of-state felony warrants, which the District Attorney will not extradite on, will be entered for Massachusetts rendition only. The remarks field should say, "will rendite Massachusetts only." – Williamstown, Ma. Police Department, 413-458-5733.

All additional, relevant sources of information (such as RMV records) will be checked prior to entering a warrant.

Warrants are to be entered as soon as all entry requirements have been satisfied.

The originals of all warrants entered into the Department's terminal will be kept in the Communications Center.

When possible, the FBI number should be included in a wanted person entry.

Caution & Medical Conditions

A caution indicator should be added to the MKEs EW, ET, or EWJ when it is known that an individual is armed and dangerous, has suicidal tendencies, has previously escaped custody, is a drug addict, or whatever is appropriate to the particular circumstances of the individual.

The reason for the caution must be entered in the MIS Field (NCIC format) or in the Caution and Medical Conditions (CMC) Field.

Persons in custody:

Upon taking a person into custody, the arresting officer will perform a CJIS/ NCIC (Q1) inquiry in order to avoid releasing a wanted or missing person. Attach the printout to the arrest report.

Complete record checks are conducted for every person placed under arrest or charged with a crime. Every folder forwarded to the court contains printouts of criminal record checks, including Board of Probation checks, queries of the Interstate Identification Index, queries of in-custody suicide threats, and pertinent Registry of Motor Vehicles records. (**CJIS regulations allow the inclusion of this statement in the WPD policy to fulfill our obligation to log CORI dissemination to another agency, without the need to complete a separate logging in the Secondary Dissemination Log)**

Suicide Risk File

Whenever a person in police custody attempts or threatens suicide at a lockup facility, the officer in charge of the lockup shall, within twenty-four (24) hours of such incident, record in the DCJIS computer the name, address and age of such person, the charge or reason for detention, and the nature and date of said attempt or threat.

Gun Inquiry

The purpose of a gun inquiry is to determine if a gun is listed in the CJIS and/or NCIC as stolen or recovered. Inquiries should be made on, but should not be limited to:

a) Confiscated guns

b) Guns in possession of arrested persons

c) Guns observed during the legal search of a premise or vehicle

d) Abandoned or found guns.

A record for a recovered (abandoned, seized, found) weapon for which no stolen or lost report is on file may be entered into CJIS.

Article File

An article, for CJIS purposes, is defined as any uniquely numbered item of property not meeting the entry criteria for any of the other property files (i.e. Vehicle, Boat, Gun, License Plate, and Securities). The definition includes, but is not limited to:

a) Office equipment

b) Color television sets

c) Bicycles

d) Household appliances

Missing persons

If a child is reported missing, a record shall be entered into CJIS immediately. The age of a missing child is anyone under the age of 21. The "Missing Person" binder in the Communication Center contains further information on entering and modifying records of missing and unidentified persons, including Amber Alerts, dental records, supplemental records, etc. Juvenile Missing Person records will be updated with medical and dental information when available within 60 days of entry. (Also see Department Policy 2.08 Missing Person)

Board of Probation

Reasons for conducting a Board of Probation (BOP) check may include, but is not limited to:

- An investigation;
- An arrest;
- An individual applying for Criminal Justice employment;
- Local licensing purposes (i.e. hawkers, peddlers, constables, and door-to-door sales people; and

- Firearms licensing purposes.

Interstate Identification Index

Interstate Identification Index (III) (QH and QR) checks may only be made for official criminal justice purposes only. These authorized purposes include:

- Criminal investigation;
- Criminal justice employment;
- Firearms licensing.

Full names are required in the "attention", "authorized" and "operator" fields of III inquiries. The use of initials, and/or the department name, is not acceptable. Each agency must be able to identify a requestor of the internal III inquiries.

Whenever III information is disseminated to another criminal justice agency, it must be logged in the agency's secondary dissemination log located in the bookcase. The log must be maintained for at least 12 months.

VIII. NATIONAL INSTANT CRIMINAL BACKGROUND CHECKS

A. SYSTEMS SURVEY (NICS)

B. NICS can only be used for Firearms Licensing purposes, no other transactions are authorized, Per the FBI, "NICS cannot 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."

IX. CJIS Extranet

Features available through the CJIS Extranet page:

SORIS – A web based Sex Offender Registration and Inquiry System.

CJIS Web Warrant Publishing – Allows a search for active and recalled Natick Police Warrant Management System warrants by name or date.

CJIS WebRMV – Allows extensive searches of RMV data, provides license images, and allows partial searches.

NexTEST – Training that is required for all users of the CJIS system every two years. Department members shall review the material presented in the "CJIS System Policy and Compliance FAQ" and then take the on-line nexTEST. Certification is valid statewide. The exam consists of 30 randomly assigned questions pulled from a pool of 200 CJIS, CORI, and FBI/NCIC policy related questions.

SWISS – Statewide Information Sharing System is designated to electronically exchange, store and facilitate the analysis of data maintained by state and local law enforcement agencies in Massachusetts.

Department Responsibilities and Resources

Annual purge of Records – Records which have reached the end of their retention period are purged from CJIS and NCIC in January. The Department CJIS Representative will remove the file folders from the Dispatch Center and forward them to the Records Division.

Monthly validation – Records which cannot be properly validated must be cancelled immediately. Validation obliges the Department to confirm that the record is complete, accurate and still outstanding or active. If upon review of the record it is determined the record is no longer valid, the record must be cancelled from CJIS and NCIC. (**See Department Policy 4.44 CJIS On-Line Validation)**

Regional working group meeting – The CJIS Representative and/or Backup Representative is required to attend the biannual Regional Working Group meetings.

Audit – Compliance audits are conducted every two to three years to verify that agencies are adhering to CJIS and NCIC policies and regulations. The purpose of the CJIS audit is to ensure that records in the system are accurate, active and timely, ensure that training is conducted, security standards are met, and to verify that the proper documentation is maintained and available for CHSB and FBI/NCIC auditing purposes. Audits occur via on-line audit program or an in-person interview. Audit records must be retained for at least one year.

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.

Offline search – This is a specialized inquiry of the CJIS and/or NCIC systems for data which is otherwise unavailable through CJIS/NCIC queries. Offline searches can be made against both active and historical records. For investigative purposes, off-line searches may be conducted to obtain data regarding a person, vehicle or property that has been the subject of a previous

CJIS/NCIC query. This data may be used to determine what specific person or workstation has run a query on the person/property of interest.

All offline search requests must be made by the agency head and submitted to the CJIS Support Unit. (See form in CJIS)

X. 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. not take CJI home or when travelling unless absolutely necessary.

XI. 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 Chief or Lieutenant, who will in turn notify the Chief and the ISO of the loss or disclosure of CJI.

3. The Chief 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.