Lunenburg Police Department

Policy Number: 4.61	Subject: Central Records
Issue Date: 11/03/2021 Revision Date(s): 1/21/2022 Effective Date: 11/03/2021	Massachusetts Police Accreditation Standards Referenced: 82.1.1; 82.1.2; 82.1.3; 82.1.6; 82.1.7; 82.2.3; 82.2.4; 82.3.5
Issuing Authority: *Chief Thomas L. Gammel*	

I. PURPOSE

This directive describes the Department's guidelines with regard to employee access to and disclosure of information contained on the Department's Records Management System (RMS). This includes incident and criminal information on the server systems (IMC), mobile data terminals in police cruisers, electronic mail messages, and information contained on the shared network. This directive also addresses records (hard copies) security, storage, and disposition.

II. POLICY

A. It is the policy of the Lunenburg Police Department to maintain IMC RMS in order to provide reliable information to be used in management decision-making.

B. The information is important for analyzing work load, determining resource needs, budget preparation, resource allocation, record keeping, employee safety and other Departmental needs. Access to data contained in the system must be controlled in a manner that will ensure only authorized access.

C. It is also necessary to permit dissemination of public data to interested individuals. This data must be in conformance with the standards of the Massachusetts Criminal History Systems Board in order that the rights of any individual are not infringed. All information needs to be carefully reviewed prior to dissemination to ensure that it is not restricted.

III. PROCEDURES

A. **Administration**: The records management system (RMS) provides a comprehensive representation of the Department's operation at any given point in time, as well as projecting future trends from current and past data.

1. The Chief of Police, the Lieutenant, or their designee shall work in collaboration with Town of Lunenburg's IT Department, and Nashoba Valley Regional Dispatch District (NVRDD) IT Department updating and maintaining the information system when needed.
2. Responsibility for recording and/or providing specific types of data is assigned to and/or shared by various shifts or Divisions. Types of data recorded into the system include, but is not limited to the following:
    a. Calls for service
    b. Arrest bookings
    c. Incident report narratives
    d. Trespass lists
    e. Stolen property
    f. Master names
    g. Offender history
    h. Collision data
    i. Juveniles
    j. Emergency notification list
    k. Alarms
    l. Business directory
    m. Street files
    n. Digital photos

B. **Records**: All arrest reports, incident reports, summons, motor vehicle violations, criminal history transcripts, digital photographs and various other records are entered in the Department's IMC RMS. These records are assigned a unique and sequential incident number. These records are password protected and may be accessed by authorized Departmental personnel from any network computer, and are available 24 hours a day. All criminal investigation reports requiring follow-up are routed to the Investigative Bureau. **[82.1.1] [82.1.7] [82.2.3] [82.2.4] [82.3.5]**

C. **Privacy and Security Precautions**: The Records Room is secured by key access. Access is limited to authorized personnel twenty-four (24) hours a day. The Chief or the Lieutenant, or their designee will be contacted for after-hours access. **[82.1.1(a)(b)] [82.1.2(c)]**

D. **Sexual Assault Records Security**: When submitting hard copies of sexual assault incident reports to the Supervisor for review, the reporting officer shall secure the sexual assault incident report in IMC. The report will be sent to the Supervisor assigned to sexual assault cases. The Supervisor assigned to review sexual assault reports will secure a copy of the report in the locked file cabinet "Sexual Assaults" located in the secured records room. The reporting officer shall

complete their initial report prior to the end of their tour of duty. Once the supervisor assigned to review sexual assault cases completes their review, they will notify a sexual assault investigator for further action.

E. **Juvenile Records Security**: Offender histories for adults and juveniles will be segregated electronically and hard copies physically. Electronic records shall be checked off as "Juveniles Involved?" under the "Incident" tab in IMC. Hard copies of closed incidents shall be filed in the Records Room. Open cases shall be filed in a locked cabinet within the Student Resource Officer's (SROs) office. Access shall be restricted by electronic key card or key to authorized personnel. Only juvenile records shall be kept in a yellow folder to distinguish them from all other records. **[82.1.2(a)]**

1. Collection of fingerprints and photographs for juvenile offenders shall be subject to same requirements as adults. **[82.1.2(b)]**
2. Dissemination of Juvenile and adult fingerprint cards, photographs and reports shall only be to other CORI approved agencies upon approval of the Chief or the Lieutenant. **[82.1.2]**
3. Retention of juvenile and adult fingerprint cards and photographs is required.
4. Juveniles taken into custody for criminal-type offenses shall be subject to the same reporting requirements as adults.

F. **Record Keeping**:

1. Written reports, photographs, and any other forms of identification shall be filed in the locked Records Room. Juvenile records will be kept physically separate from adult arrest records. Juvenile reports in the RMS system shall be restricted to authorized personnel only. **[82.1.2(b)]**
2. Disposition of Juvenile Records: When a juvenile reaches adult age, any records of activity obtained while as a juvenile will remain with any adult record of such individual. **[82.1.2(d)]**
3. Expungement by the Court: This procedure shall apply to juvenile and adult records.
    a. Upon receipt of a judicial order of expungement of any record, records management personnel shall identify and obtain the record.
    b. Hard copies shall be destroyed by shredding or burning.
    c. Electronic records, files and other data will be deleted manually or using specific expungement or deletion software programs in the Department's IMC RMS.**[82.1.2(e)]**

G. **Releasing of Department Records**: **[82.1.7]**

1. GENERAL PUBLIC: Members of the public requesting access to Department records shall submit a written request form to the Records Access Officer (RAO). The RAO shall approve requests for dissemination. The RAO will disseminate records in accordance with the state public records law and with the Criminal Offender Records Information Act (C.O.R.I). **[82.1.1(c)]**
2. Due to changes in the Public Records Law, the Lunenburg Police Department is required to change the way it responds to public records requests concerning reports of sexual or domestic violence. With the exception of the

Records Clerk, no other Department member shall release records to the public without authorization from the Chief of Police or the Lieutenant. If a request to release Department records is made the RAO shall remove the following records prior to providing the documents to the requesting party:

a. All reports of rape and sexual assault
b. All reports of attempted rape and sexual assault
c. All reports of abuse perpetrated by family or household members
d. All communications between police officers and victims of rape, sexual assault, or abuse perpetrated by family or household members
e. Any police log(s) concerning such reports

3. POLICE DEPARTMENTS/ OUTSIDE AGENCIES: A request received by phone for records from a Police Department or outside agency the Shift Supervisor is to call back that department or agency and confirm the identity of the caller before the release of any records. After confirmation is made the Shift Supervisor may disseminate records to any other criminal justice agency appearing on the CORI list in CJIS and any other authorized agency. **[82.1.1(c)]**

H. **Photographs**: Photos are stored both electronically in the RMS and in the Records Room. Photographs in the RMS are password protected, and hard copies are secured in the locked Records Room.

I. **Equipment, Hardware, Software and Systems**:

1. Adding / Modifying Software & Hardware: No one may add or modify software or hardware without the authorization of the Chief of Police and System Manager(s).

J. **Licensing**: All programs introduced into the system shall be properly licensed.

K. **Computer Access / Security**: Software and hardware have been installed to prevent unauthorized network access. The System Manager(s) will assign access logins and the initial user's passwords for the Department computer network system: **[82.1.6(c)]**

1. Passwords are encrypted and are known only to the users and System Manager(s).
2. Users may not divulge their passwords to anyone without the authority of the System Manager(s).
3. Access codes will be audited to verify all logins.
4. Logins will be audited annually for verification of all passwords, access codes and access violations. **[82.1.6(d)]**
5. Logins no longer needed shall be disabled on the system server.

L. **Computer File Backup & Storage**:

Records on the Department's centralized computer system shall be backed up onto a media device daily by System Manager(s). The back-up media device shall be stored in a safe location. **[82.1.6(a); 82.1.6(b)]**

M. **Use of Department E-Mail & External Internet Services**:

All internal e-mail messages whether sent or received by employees and all files located or accessed by departmental computers are considered Department records. All external files, including personal e-mails and data that are accessed using departmental computers are not considered private communications, and can be subject to scrutiny and/or disclosure by proper departmental or legal authority.

IV. RECORDS RETENTION SCHEDULE

The Department shall comply with the Commonwealth of Massachusetts Municipal Records Retention Manual 2019 edition. See hyperlink: https://www.sec.state.ma.us/arc/arcpdf/MA_Statewide_Records_Schedule.pdf. **[82.1.3] [82.3.5]**