Lexington Police Department	**Subject:** **Computers, Record Security & General Management** **Accreditation Standards:** Reference: 11.4.4; 82.1.6; 82.1.7	**Policy Number:** 13A **Effective Date:** 12/1/11

☐New ☒Revised	**Revision Dates:**	1/24/19	5/31/20				

By Order of: Mark J. Corr, Chief of Police

The Municipal Police Institute, Inc. (MPI) is a private, nonprofit charitable affiliate of the Massachusetts Chiefs of Police Association. MPI provides training and model policies and procedures for police agencies. This policy is an edited version of MPI Policy 4.21, "Computers and Data Security."

GENERAL CONSIDERATIONS AND GUIDELINES

The Lexington Police Department utilizes computer equipment to aid in accomplishing its primary mission: responding to calls for service, preventing crime, apprehending criminals and documenting incidents. Computers and access to databases supplied by the Department or Town make our work more efficient and more accurate.

The Department has a central computer with a police information management system called "PROPHOENIX". The Department also utilizes a computer system "PMAM", a policy and training module accessible on-line. The Department also has access to the Town's network server for internet, Microsoft Office®, and e-mail. Extensive on-line records are accessible to Department personnel 24 hours a day, seven days a week. The computerized records include:

- All calls for police service, dispatch logs, arrest logs;
- Restraining orders;
- Motor vehicle citations;
- Arrest and police information records;
- Police incident reports;
- Personnel information;
- Statistical and data summaries; and additional police and management records.

Most of the Department's administrative reporting is conducted within the central computer system. All other reports will be prepared in accordance with Department procedures on forms approved by the Chief of Police

This policy will serve as a guide to help all employees preserve the integrity of our data, manage use of computer systems, decrease liability exposure, and prevent unlawful or wrongful actions involving computers and data.
This policy supplements the policies and user agreements of state and federal data providers such as Leaps/NCIC/CJIS and contracted databases, in addition to the Electronic Communications Policy for Town of Lexington employees.

It is the policy of the Lexington Police Department to:

1. Utilize computer resources to enhance our ability to perform our mission; and,

2. Improve officer safety through the availability of information, while maximizing security protocols and system integrity.

PROCEDURES

DEFINITIONS:

Hardware: The tangible components of a computer such as disk drives, monitors, keyboards, mouse, etc.

RMS: Records Management Systems of this Department and others.

Offensive/Disruptive Communications: Communications which contain sexual content or sexual implications, racial slurs, gender-specific comments, or any other content that offensively addresses a person's race, creed, religion, physical or mental disability, color, sex, national origin, age, occupation, marital status, political opinion, sexual orientation, or any other group status.

Password: A word or string of alphanumeric characters restricting access to an account, network, database, or file to an authorized member.

Software: The programs, data, routines, and operating information used within a computer.

Virus: A hidden code within a computer program or file intended to corrupt a system or destroy data stored in a computer.

Malware: Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

System Administrator: An individual assigned or authorized by and under the direction of the Chief of Police to oversee and/or manage the operation and security of the department computer system and network

A. COMPUTER PROTOCOLS

1. Central Computer System / PROPHOENIX

a. The central computer system shall be the principal depository for police information. This information is protected by a multi-level security system, which includes:

i. Employee passwords and identification numbers;
ii. Security levels which are assigned by rank or position; and
iii. Terminal access; certain information may not be accessible unless a specific terminal is used.

b. Computer Use and Accountability

i. The computer will only allow access when an ID number is used in tandem with the correct employee password. Once access is obtained, the computer will "stamp" any new information (or changes to existing information) with the employee ID number.
ii. Personnel shall be responsible for any computer information "stamped" with their ID number. Each person is responsible for logging off.

c. Authorized Users

i. The job of protecting the hardware, software, and data from abuse is shared by all users of the Department's data processing systems. The potential for someone (citizen or employee) to suffer a loss or inconvenience due to improper or inappropriate use of the Department's data processing systems is real, whether malicious or accidental.
ii. Only authorized users may have access to the Department computer system. Authorized users shall have an individual user account arranged by the System Administrator.
iii. The use of Department computer systems and equipment is solely for purposes authorized by the Department. Unauthorized use is a violation of these policies and procedures, and violators may be subject to disciplinary action.

d. It is important for all personnel to maintain a working knowledge of the computer system as required by the employee's duties and responsibilities.
e. Commanding Officers and Supervisors shall:

i. Monitor the computer skills demonstrated by employees under their supervision;
ii. Whenever possible, provide basic and remedial training; and
iii. Identify employees requiring advanced or specialized training from a computer administrator.

f. It shall be the responsibility of all personnel to enter information into the computer system **accurately** and in accordance with Department guidelines.
g. Department Employees will be issued a **Microsoft Outlook** account for the purposes of communicating with:
h. Department Employees;
i. Town employees, and
j. Other individuals necessary to achieve departmental goals.
k. Any employee assigned a network account with the Town of Lexington will, prior to access the network, sign the Town of Lexington's computer policy and adhere to the guidelines contained therein.

2. Software

a. Generally

i. All software programs installed or introduced onto Department computers must be authorized by the System Administrator.
ii. Software used in the Department's computer systems is property of the Department and will not be used, copied or distributed without permission of the System Administrator.

b. Unauthorized Software [11.4.4]

i. Members are strictly prohibited from installing software programs, which have not been authorized for use by the System administrator or Designee. Any unauthorized software, such as games and other personal amusement software, will be deleted.
ii. No employee shall install or use software on Department computers that is unlicensed, in violation of the software licensing agreement, or has been copied in violation of the law.
iii. No employee shall introduce unauthorized programs or manipulate or alter programs running on mobile network computers or desktop computers.

3. Data Files

a. Generally

i. Employees must use caution when introducing data files into Department workstations. Data should be downloaded or received only from a trusted source.
ii. Opening of suspect files for investigatory purposes should be done on designated investigative workstations only. The workstations are not connected to the Department network.
iii. All disks and external storage devices, including disk drives (i.e., thumb drives), will be scanned by the user for viruses when introduced into any Department computer. This can be

accomplished by right-clicking on the appropriate drive letter in the My Computer menu and choosing the option "Scan for Viruses" on the drop-down menu.

iv. The Department will maintain proprietary rights over any work generated by its members in the course of their duties, and software or files will not be sold, distributed or maliciously deleted without permission of the Chief of Police. The use and distribution of such files will be at the discretion of the Chief or the System Administrator.

b. Prohibited

i. Employees shall not introduce unauthorized data files into mobile network computers, handheld devices or desktop computers from any source including floppy disks, CDs, DVDs, thumb drives, or any other media or on-line sources. **[11.4.4]**

ii. Employees shall not encrypt data, or change permissions or files, without the formal approval of the Chief of Police or the System Administrator.

4. Data Back-ups

a. Generally

i. Daily backup of data shall be accomplished by the A-shift Commanding Officer for each A-shift and the back-up media stored in a secure location. **[82.1.6(a)]**

ii. Weekly backup of data shall be accomplished by the Monday A-shift Commanding Officer.

b. Media Storage **[82.1.6(b)]**

i. Daily back-up media will be stored locally in the fire retardant safe located in the computer server room.

ii. The weekly backup will be placed in the CO's office portable fire retardant safe. In the case of an emergency and the building must be evacuated the safe in the CO's office will be taken by the CO upon evacuation.

c. Data

i. Data files (word processing, e-mail, and spread sheets) will be backed up if they are stored on the department server. Backup of data not stored on the server is the responsibility of each user. The Department cannot be held responsible for lost data due to system failure caused by power outages or other problems that may cause unexpected shut down. If data is important to a user, s [he] must back it up.

ii. Mobile computer network transaction logs of CJIS queries and responses must be maintained pursuant to 3.8.1 of the CJIS User Agreement. Files must be maintained for at least two years and must be available to CHSB upon their request. All other MDT log files shall also be stored for at least two years.

d. MEDIA DISPOSAL: Back-up media which is no longer serviceable or which contains data that is no longer to be stored must be destroyed, so that the data cannot be retrieved, before being discarded.

5. Application Security

a. Computer system security is the responsibility of all users. Employees may use Department computer systems only for Department purposes
b. User access will be limited to only those programs, applications, records, and data necessary for that user to perform his/her assigned tasks. Users may access such records only for department business. **[82.1.7]**
c. User Passwords

i. Each authorized user of the system will be issued a login name and password. Users are responsible for maintaining the security of their passwords and should never share them with anyone, including other employees. **[82.1.7]**
ii. All personnel should change their password annually as directed and/or when system administrator advises of a need to change.
iii. Any person may request an immediate password change if the confidentially of their password has been compromised.
iv. The appearance of passwords on terminal screens and printouts is suppressed.
v. No employee shall log into any computer or application using the username and password of another employee. This action is a crime under M.G.L. c. 266 s. 120F and is a serious breach of security.[i]

d. Role of Program Administrators

i. Program administrators are persons who may be assigned to manage a particular software program or application by the Chief of Police.
ii. They shall manage and be responsible for user accounts, passwords, access, resets, and audits for their particular program.
iii. Program administrators shall ensure that only current, authorized users are allowed access to their program or application.

6. Network Security **[82.1.6(c)]**

a. Network security is a critical security issue.

b. Servers and routers are located in a secure area to avoid physical, illegal, and unauthorized access to this hardware.
c. The Department shall provide various layers of security to safeguard data and software from unauthorized access. These security measures include:

    i. Detection of illegal penetration of the network and prevention of unauthorized access to the network and servers;
    ii. Prevention of unauthorized access to stored data;
    iii. Up-to-date anti-virus software installed and running on all servers and clients;
    iv. Minimal network administrator accounts and high security of network administrator passwords; and
    v. Secure setting for routers and firewalls.

d. Supervised access to the network by vendors, maintenance technicians, and contractors may be allowed on an as-needed basis and only with permission of the Chief or the System Administrator.
e. Access to the Department's network will be limited to those with a legitimate need to use the system to access or input data.
f. User access will be limited to only those programs and data necessary for that user to perform his/her assigned tasks.
g. Each authorized user of the system will be issued a network login name and password. Users are responsible for maintaining the security of their passwords and should never share them with anyone, including other employees.
h. A user's password must be immediately changed if it becomes known to others. All user passwords should be changed bi-annually.
i. All user passwords will be changed whenever a security infraction has been discovered.
j. The appearance of passwords on terminal screens and printouts is suppressed.
k. A network password audit shall be conducted annually by Chief of police or Designee. **[82.1.6(c)]**

7. Employee Activity

a. PROPHOENIX

    i. All Department employees shall be trained in the use of PROPHOENIX. The training shall include how to access the system, write reports, enter property, view time management, etc.
    ii. It shall be the responsibility of the employee to view his/her time management to make sure all time is accurate.

b. E-MAIL/Microsoft Outlook

i. All Department employees shall be trained in the use of the e-mail system. This training shall include how to access e-mail, create e-mail messages, open an attachment, attach a document, send and receive e-mail and manage an e-mail account.

ii. It shall be the responsibility of each employee to check their E-mail at least once per working shift and to read all e-mail messages, and their attachments, received from Department personnel.

iii. Written directives may be distributed to employees by e-mail. Once the mail is opened, it shall be understood that the directive has been formally issued to the officer. The e-mail receipt indicating that the employee received and opened the e-mail shall serve as a record that the employee received and reviewed the written directive.

iv. Any e-mail that is time-stamp delivered but has no date/time as to when it was opened shall be considered unread. If the message has no opened date/time and it does not exist in the recipient's mailbox, then it is considered to have been deleted, without being read, by the recipient.

v. No employee shall delete any Department related e-mail without first opening it and reading the e-mail and/or its attachments.

vi. The e-mails of Department employees are considered public record unless the content falls under a statutory exemption.[ii] E-mails containing jokes or personal comments to others will likely be deemed a public record (M.G.L. Chapter 66 § 10).

vii. The following types of e-mail activities are expressly prohibited

a) Transmission of global or mass mailings unless related to department business or unless prior authorization has been received from the Chief or his/her Designee.
b) Transmission of chain letters or virus alerts.
c) Transmission of any e-mail containing abusive, harassing, discriminatory, or sexually explicit language or content.
d) Transmission of deceptively labeled e-mails, to include any e-mail that carries a misleading subject line, is anonymous, is attributed to another person, or identifies its true sender incorrectly.
e) Inclusion of C.O.R.I. information within any e-mail, except where the recipient's e-mail address has been previously confirmed to be a legitimate and secure reception point.
f) Any other transmissions or inclusions that violate federal, state, or local law.

c. Internet Access

i. Internet access is available to employees for legitimate business purposes only.
ii. Users shall not use the Department system to access, download, upload, store, print, post, or distribute pornographic, obscene, or sexually explicit materials.
iii. Users may visit an otherwise unacceptable site if it is for a legitimate law enforcement purposes and only with authorization of a supervisor.
iv. If an employee accidentally accesses an unacceptable site, the employee must immediately disclose the incident to a supervisor. Such disclosure may serve as a defense against an accusation of an intentional violation of this policy.

d. Release of Department Records **[82.1.7]**

i. Records, including records containing criminal history data, may be released only in accordance with Massachusetts Law and Department policy.
ii. Data maintained or obtained by this Department shall not be distributed in violation of investigative confidentiality or C.O.R.I through e-mail or uploading to chat (Officer.com) or entertainment sites (i.e., Break.com, Rotten.com, etc.). Data may be distributed for legitimate law enforcement purposes only.

8. Computers and Media Evidence

a. Cautions

i. Opening files of evidence hard drives and computer media may change data and file use markers, changing and/or contaminating evidence.
ii. Media from questionable origin may introduce viruses or malware into the department network.
iii. Electronic Media will be searched only with authorization from the court in conjunction with the Office of the District Attorneys and/or the NEMLEC Computer Crime Unit.

b. See the Department Policy ***83A - Collection and Preservation of Evidence*** prior to opening or viewing files on evidence hard drives or other media.

B. ADMINISTRATIVE REPORTING

1. **Daily Log**. A daily log, in accordance with M.G.L. Chapter 41, section 98F, shall be maintained and shall record:

a. All calls for service, complaints and reported crimes;
b. Type and location of incident or call;

c. When appropriate, the complainant (when identified);
d. Case number and action code;
e. The units assigned; and
f. An arrest log listing the names and addresses of any person arrested and the applicable charges.
g. **Public Record.** The public daily log unless otherwise provided by law, is public information and shall be made available to the public without charge, during regular business hours and at all other reasonable times. Daily Log and arrest entries exempt from public record as required by law will be marked not for public in the Pro Phoenix CAD entry system.

2. **Formal Police Reports**. As required by the Chief of Police, all formal police reports shall be entered into the computer by the responding officer(s) in addition to a journal entry.

a. Commanding Officers may, at their discretion, require a report in any situation.
b. Commanding Officers shall review all reports entered by officers and personnel under their command (or working during the duty shift).
c. Final report review and inspection will be the responsibility of the designated Report Review Officer.

3. **Monthly Reports**. The following reports shall be prepared monthly by clerical staff assigned by the Chief of Police or designee:

a. Motor vehicle accident summaries;
b. Citations - moving motor vehicle violations;
c. Police fleet maintenance, mileage and fuel consumption. To be handled by the Police Mechanic.
d. Note: The Chief of Police may require monthly reports from any of the Department's organizational components.

4. **Annual Reports**. Police annual reports shall be prepared as follows:

a. The annual National Incident Based Crime Reporting System (NIBRS) shall be prepared by clerical staff. This report shall be a summary of the twelve monthly crime reports for the calendar year.
b. The Annual Report of the Police Department to the Town of Lexington shall be prepared by the Chief of Police or by a designee under the Chief's direction. It shall include a summary of department activities, accomplishments, concerns and problems encountered during the year.
c. A traffic enforcement report identifying the high accident locations in Lexington and outline a program for suppressing hazardous driving behaviors.
d. An International City/County Management Association (ICMA) annual report on performance measures.

5. **On-line Computer Reports**. The central computer system is capable of generating numerous summary reports for any given date range. These reports will give department personnel (particularly Commanding Officers and heads of Department components) the ability to:

   a. Identify crime or incident trends;
   b. Summarize significant occurrences for any given time period;
   c. Keep personnel informed of major crimes, accidents, arrests or other important activities;
   d. Review statistical summaries for the purpose of allocating and distributing department resources; and
   e. Identify objectives for future programs.

C. REPORT FORMS

1. The Captain of Administration shall be responsible for maintaining a system of accountability for all Department report forms.

2. All forms shall be approved for use by the Chief of Police.

3. REPORT FORMS – G-DRIVE. All approved report forms shall be retained on the police departments 'freedom' (G :) drive, under forms and documents. A copy of all approved forms will also be labeled and placed in a three ring binder in the CO's office containing the following information:

   a. The date the form was created.
   b. Instructions for the proper use of each form.

4. New Report Form Requests

   a. Any request for a new report form must be submitted to the Captain of Administration. Each request should include the reasons why the form is needed and suggestions regarding format and use.
   b. When a new form is deemed necessary, a design shall be prepared under the direction of the Captain of Administration.
   c. New report forms will be circulated to the command staff in accordance with staff review procedures.
   d. All new report forms shall be subject to the approval of the Chief of Police.
   e. New report forms shall be placed on the G-Drive and a copy inserted into the master book of report forms with instructional material outlining the proper use of the form.

5. At least once each year, all existing forms shall be reviewed, amended, and/or deleted from the report form system by the Captain of Administration.

D. MANDATORY REPORTS

1. The Chief of Police, or a designee, shall ensure that periodic reports, reviews, and other activities mandated by the accreditation standards are accomplished.

2. The Accreditation Manager shall:

   a. Maintain a list of all activities, which are mandated by the accreditation standards;
   b. Distribute, on an annual basis, a list of all mandatory reports to the affected personnel;
   c. Receive a copy of all mandatory reports, reviews and other materials; and
   d. Bring to the attention of the Chief of Police, or his designee, any report, review or other material, which has not been completed in a timely manner.

---

[i] M.G.L. c. 266, §120F.

[ii] M.G.L. c. 4, §7.