COMPUTERS AND DATA SECURITY

POLICY & PROCEDURE NO. **4.21**	ISSUE DATE: ____05/22/17
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **11.4.4; 82.1.6; 82.1.7**	EFFECTIVE DATE: ____05/22/17
	REVISION DATE: _____

I. GENERAL CONSIDERATIONS AND GUIDELINES

This 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 this department make our work more efficient and more accurate.

With the use of computers as a communications tool, what took days or weeks to do a few years ago can now be done in minutes. E-mail, live scan fingerprinting, digitized images, audio and video can quickly put high quality records into the hands of employees.

This technological advantage does not come without its own pitfalls. Misplaced media may result in the loss of a high volume of confidential data. A confidential image, casually forwarded, could end up in the mail boxes of thousands of recipients or displayed on internet entertainment web sites. Hackers may enter systems and access, change or destroy data. Viruses can enter the system via innocent files such as internet images and games, and then wreak havoc on system operability, steal data or passwords, or allow unauthorized users to access the system.

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.

II. POLICY

It is the policy of this 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.

III. DEFINITIONS

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

B. *RMS*: Records Management Systems of this department and others.

C. *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.

D. *Password:* A word or string of alpha-numeric characters restricting access to an account, network, database, or file to an authorized member.

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

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

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

H. *System Manager:* 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.

IV. PROCEDURES

A. Authorized Users

1. 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.

2. Only authorized users may have access to the department computer system. Authorized users shall have an individual user account provided by the System Manager.
3. 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.

B. Software

1. GENERALLY
   a. All software programs installed or introduced onto department computers must be authorized by the System Manager.
   b. 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 Manager.
2. UNAUTHORIZED SOFTWARE [11.4.4]
   a. Members are strictly prohibited from installing software programs which have not been authorized for use by the System Manager. Any unauthorized software, such as games and other personal amusement software, will be deleted.
   b. 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.
   c. No employee shall introduce unauthorized programs or manipulate or alter programs running on mobile network computers, handheld devices or desktop computers.

C. Data Files

1. GENERALLY
   a. Employees must use caution when introducing data files into department work stations. Data should be downloaded or received only from a trusted source.
   b. Opening of suspect files for investigatory purposes should be done on designated investigative work stations only. The work stations are not connected to the department network.
   c. 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.

d. 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 Manager.

2. PROHIBITED

a. 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]

b. Employees shall not encrypt data, or change permissions or files, without the formal approval of the Chief or the System Manager.

D. Data Back-ups

1. GENERALLY: Regular backup of data shall be accomplished by department's CJIS representative, and the back-up media stored in a secure location. [82.1.6(a)]

2. MEDIA STORAGE [82.1.6(B)]

a. Daily back-up media will be stored locally by the department's CJIS representative.

3. Back-up media may also be stored off-site.

4. DATA

a. 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.

b. 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.

5. 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.

E. Application Security

1. Computer system security is the responsibility of all users. Employees may use department computer systems only for department purposes.
2. 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]
3. USER PASSWORDS
   a. 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.
   b. A user's password must be immediately changed if it becomes known to others.
   c. All user passwords will be changed whenever a security infraction has been discovered.
   d. The appearance of passwords on terminal screens and printouts is suppressed.
   e. 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.[1]
4. ROLE OF PROGRAM ADMINISTRATORS
   a. Program administrators may be assigned to manage a particular software program or application by the Chief of Police.
   b. They shall manage and be responsible for user accounts, passwords, access, resets, and audits for their particular program.
   c. Program managers shall ensure that only current, authorized users are allowed access to their program or application.

F. Network Security [82.1.6(c)]

1. Network security is a critical security issue.
2. Servers and routers shall be located in a locked or secure area to avoid physical, illegal, and unauthorized access to this hardware.

3. The department shall provide various layers of security to safeguard data and software from unauthorized access. These security measures include:
   a. Detection of illegal penetration of the network and prevention of unauthorized access to the network and servers;
   b. Prevention of unauthorized access to stored data;
   c. Up-to-date anti-virus software installed and running on all servers and clients;
   d. Minimal network administrator accounts and high security of network administrator passwords; and
   e. Secure setting for routers and firewalls.
4. 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 Manager.
5. Access to the department's network will be limited to those with a legitimate need to use the system to access or input data.
6. User access will be limited to only those programs and data necessary for that user to perform his/her assigned tasks.
7. 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.
8. A user's password must be immediately changed if it becomes known to others. All user passwords will be changed whenever a security infraction has been discovered.
9. The appearance of passwords on terminal screens and printouts is suppressed.
10. A network password audit shall be conducted annually by department's CJIS representative. [82.1.6(c)]

G. Employee Activity

1. E-MAIL
   a. 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.
   b. It shall be the responsibility of each employee to check the department's e-mail at least once per working shift and to read all

e-mail messages, and their attachments, received from department personnel.

c. 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. For further information, see the department policy on ***Written Directives.***

d. Any e-mail that is time- stamped-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.

e. No police officer shall delete any department related e-mail without first opening it and reading the e-mail and/or its attachments.

f. The e-mails of department employees are considered public record unless the content falls under a statutory exemption.[2] It is unlikely that e-mails containing jokes, obscene images, or personal comments to others will fall under one of the statutory exemptions.

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

1) Transmission of global or mass mailings unless related to department business or unless prior authorization has been received from the Chief or department's CJIS representative.

2) Transmission of chain letters or virus alerts.

3) Transmission of any e-mail containing abusive, harassing, discriminatory, or sexually explicit language or content.

4) 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.

5) 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.

6) Any other transmissions or inclusions that violate federal, state, or local law.

2. INTERNET ACCESS

a. Internet access is available to employees for legitimate business purposes only.

b. Users shall not use the department system to access, download, upload, store, print, post, or distribute pornographic, obscene, or sexually explicit materials.

c. Users may visit an otherwise unacceptable site if it is for a legitimate law enforcement investigation and only with authorization of a supervisor.

d. 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.

3. PROHIBITED: Instant messaging software, movies, music sharing software or other peer to peer data sharing software are prohibited.

4. RELEASE OF DEPARTMENT RECORDS [82.1.7]

a. Records, including records containing criminal history data, may be released only in accordance with department policy. See the department policy on ***Records Requests***.

b. 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.

H. Evidence Computers and Media

1. CAUTIONS

a. Opening files on evidence hard drives and computer media may change data in the files and file use markers, changing and contaminating evidence.

b. Media from questionable origin may introduce viruses or malware into the department network.

2. See the department policy on ***Collection and Preservation of Evidence*** prior to opening or viewing files on evidence hard drives or other media.

[1] M.G.L. c. 266, §120F.

[2] M.G.L. c. 4, §7.