Somerville Police Department	TYPE: GENERAL ORDER	POLICY NUMBER: 407	VERSION: 2.00
	Subject: **Computers, Data Security and Mobile Devices**		
	Issuing Authority: **Charles Femino, Chief of Police**	Signature: Charles J Femino Number of Pages: Page 1 of 10	Effective Date: December 23, 2021
Accreditation Standards (5th Edition) 11.4.4, 41.3.7, 81.2.10, 82.1.6, 82.1.7	☐ New ☒ Revised ☐ Amended		

Revision & Reissued Dates:	5/22/2015						

Purpose

The Somerville Police Department uses 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 make our work more efficient and more accurate.

With the use of computers, what took days or weeks now takes minutes. Email, live-scan fingerprinting, digitized images, audio, and video can quickly put high quality records into the hands of employees.

Technology does not come without its 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 websites. Hackers can enter systems and access, change, or destroy data. Viruses can enter the system via innocuous files like images and games, and 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 and wrongful actions involving computers and data.

Policy

It is the policy of the Somerville Police Department to:

1. Use computer resources to enhance our ability to perform our mission.

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

Definitions

Hardware: The tangible components of a computer like disk drives, monitors, and keyboards.

RMS: Records Management Systems of this department and others.

Offensive/Disruptive Communications: Communications which contain sexual content or sexual connotations, 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 alpha-numeric 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 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.

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 by malicious or accidental means.

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, like games and other personal amusement software, will be deleted. [41.3.7(a)]

b. No employee shall install or use software on department computers that is unlicensed, in violation of the software licensing agreement, or which 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. [41.3.7(b)]

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 and flash drives, will be scanned by the user for viruses when introduced into any department computer. This can be done by right-clicking on the appropriate drive letter in the My Computer menu and choosing the option "Scan with Malwarebytes' Anti-Malware" 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 the permission of the Chief of Police. The use and distribution of these files will be at the discretion of the Chief or the System Manager.

2. Prohibited

a. Employees shall not transfer or introduce unauthorized data files into city owned mobile network computers, handheld devices, or desktop computers from any source

including: CDs, DVDs, external drives, or any other media or on-line sources. [11.4.4; 41.3.7]

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

D. Data Back-ups

1. Generally: Regular backup of data shall be accomplished by the System Manager and the back-up media will be 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 on the back-up server in the server room.

3. Data

a. Data files (word processing, email, 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, he/she 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 (2) years and must be available to CHSB upon their request. All other MDT log files shall also be stored for at least two (2) years.

4. 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 after 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 data 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. All user passwords shall be changed at least once per year.

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 Mass. Gen. Laws Ch. 266 Sec. 120F and is a serious breach of security.

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.

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 of Police 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 password security and should never share a password with anyone.

8. A user's password must be immediately changed if it becomes known to others. All user passwords shall be changed at least once per year.

9. All user passwords will be changed whenever a security infraction has been discovered.

10. The appearance of passwords on terminal screens and printouts shall be suppressed.

11. A network password audit shall be conducted annually by the System Manager, or his/her designee. [82.1.6(d)]

G. Employee Activity

1. Email

a. An SPD issued Email account should be used for business purposes only. In limited situations, employees may use a department issued Email account for personal reasons, but employees should be advised, all information transmitted via an SPD issued email account is subject to the public records laws. The use of an SPD issued email account strictly for union business is authorized.

b. All department employees shall be trained in the use of the email system. This training shall include how to access email, create email messages, open an attachment, attach a document, send and receive email, and manage an email account.

c. It shall be the responsibility of each employee to check the department's email **at least once per working shift** and to read all email messages, and their attachments, received from department personnel.

d. Any email 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 employee shall delete any department related email without first opening it and reading the email and/or its attachments.

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

g. The following types of email 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 of Police, or his/her designee.

(2). Transmission of chain letters or virus alerts.

(3). Jokes

(4). Inappropriate social commentary.

(5). Transmission of any email containing abusive, harassing, discriminatory, or sexually explicit language or content.

(6). Transmission of deceptively labeled emails, to include any email that carries a misleading subject line, is anonymous, is attributed to another person, or identifies its true sender incorrectly.

(7). Inclusion of C.O.R.I. information within any email, except where the recipient's email address has been previously confirmed to be a legitimate and secure reception point.

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

2. Internet Access [81.2.10]

a. Internet access is available to employees for legitimate business purposes only. Internet access used strictly for Union business is authorized.

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. This 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. See the department policy on Social Networking.

4. Inappropriate use of department computers, email and/or the improper use of the Internet is in violation of department policy and may result in disciplinary action, up to and including termination of employment.

5. 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 424 - Report Management and Dissemination.

b. Data maintained or obtained by this department shall not be distributed in violation of investigative confidentiality or C.O.R.I through email or uploading to chat or entertainment sites. 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 Evidence Collection prior to opening or viewing files on evidence hard drives or other media.

I. Department Issued Mobile Devices [81.2.10]

1. For many positions within the Somerville Police Department, the use of a mobile electronic device is a cost effective solution to facilitate quicker and improved communications between department personnel. Under certain circumstances, the department may choose, at their own discretion, to supply employees and/or contractors, with mobile electronic devices. These devices shall remain the property of the Somerville Police Department and shall be restricted to the uses set forth in this section.

2. Issuance of Mobile Electronic Devices

a. It is the sole discretion of the Somerville Police Department what types of devices, if any, are issued to an employee. Prior to receiving a department issued smart phone, employees must return their presently assigned cell phone to the city telecommunications unit.

b. Prior to receiving a department issued mobile electronic device, employees must review the regulations set forth herein and complete any training provided by the department. Employees must also agree to and sign the attached Terms of Acceptance Form.

c. Employees issued a mobile electronic device shall not have any expectation of privacy in anything created, stored, sent or received on a department issued mobile electronic device. All information stored on these devices is subject to a Freedom of Information Act request from the public. Employees are reminded, the mobile electronic device remains the property of the department.

d. It is incumbent upon all employees to ensure that the system software and application updates are kept current. Users will be notified of available updates directly on the device and must follow instructions for downloading and updating the device.

3. Damaged/Lost or Stolen Mobile Electronic Device

a. If your department issued device is damaged in the course of business, the device must be brought to the telecommunications office located in City Hall for repair/replacement. In addition, the damaged device and the reasons for such damage must be reported to your supervisor immediately.

b. Lost or Stolen equipment must be reported immediately to your supervisor and the telecommunications department so that service can be cancelled on the device.

4. Return of Mobile Electronic Equipment

a. Upon resignation or termination of employment, or at any time upon request by the Department, the employee must produce the equipment for return or inspection. Employees, who are unable to present the equipment back to the city in good working condition because of misuse or neglect, may be subject to provide the cost of a replacement.

b. Employees are also required to ensure that all outstanding costs for equipment loss, damage or unauthorized charges are paid in full prior to separating from employment.

5. Mobile Device Usage

a. The use of a department issued mobile electronic device for personal reasons should be limited. Employees are prohibited from using a Department-issued mobile device for non-work related purposes , including, but not limited to, spending excessive

amounts of time on the internet, playing games, or otherwise creating unnecessary network traffic.

b. Material that is fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by any form of electronic communication or displayed on or stored in a Department-issued cell phone (or other device). Users encountering or receiving this kind of material should immediately report the incident to their supervisor.

6. Text Messages and Emails

a. Employees that are provided a Department-issued mobile device are discouraged from using the text message capabilities for communication regarding ongoing investigations. In the event that text messages and/or emails are sent and/or received relative to an investigation, that employee is prohibited from deleting the substance of the communication from the Department-issued cell phone.

7. Camera and Video Capabilities

a. Employees should be aware that any photographs and/or video taken with a Department-issued mobile device may be subject to discovery obligations that require the production of these materials. Employees must preserve any such photographs and/or video evidence prior to deleting them from the device.