SPRINGFIELD POLICE DEPARTMENT

Standard Operating Guideline

Effective Date: 04/04/2017	Supersedes Policy Dated: 06/30/2012	Rescinds:	SOG Number: 308.1
Accreditation Index: 82.1.6			
Part Title: Support Services	**Chapter Title:** Information Systems Management [1]		
Chief of Police:			

Information Systems

I Policy

The Springfield Police Department utilizes a variety of computer systems in providing services to the community. All employees shall be trained in the use of various computer systems and shall exercise the utmost level of integrity with all computers, local networks, and non-local networks.

Computerized networks include but are not limited to the Missouri Uniform law Enforcement System (MULES), Springfield Greene County E-911 (CAD), City Utilities Customer Information System, Information Systems (City Departments and Police Network), Records Management System (RMS), and the Internet.

II Definitions [2]

Application Password – A password that a user may assign within an application to prohibit other users from opening the secured application.

Hardware – Computer components which include processor, keyboard, monitor, printer, mouse, cables, connectors, adapters, telephones, and any other device attached to any component.

Network – System of connected devices (computers, printers, etc.) which communicate and share services.

1 Chapter Title revised, typographical correction, per Policy Change Order 17-014.
2 Definitions revised, capitalization changes and minor rewording for consistency, PCO 17-014.

Network Password – A code usually consisting of alpha and numeric characters that a user utilizes to gain access to a network.

Personal Computer (PC) – A stand-alone computer system.

Personally Owned Laptop – A laptop computer owned by the employee and authorized to be used for City business.

Power on Password – A password assigned to the hardware of a PC that prevents other users from starting the system.

Software - Any removable magnetic media, floppy disk (diskette), tape, or program that resides on or can be copied to removable magnetic media for use in or written in a computer readable language.

System Administrator - The individual responsible for operating and maintaining the department's computer network system.

Workstation - Desktop or laptop computer which is connected to the network. Workstations give the user access to network services.

III Procedure [3]

1 LEGAL OBLIGATIONS

1.1 Use of an electronic computer is subject to all federal, state, and local law, including: [4]

1.1.1 RSMo 569.095 - 569.099 concerning computer crime. [5]

1.1.2 RSMo 573.010 - 573.065 concerning pornography and related offenses.

1.1.3 The Missouri Sunshine Law, RSMo 610.029.

1.2 Personally owned laptop computers, when used for City business, are subject to the same policies.

2 SUPERVISOR RESPONSIBILITY

2.1 Makes request to Information System Division, Communications Department or responsible agency for employee accounts, training, and certification.

2.1.1 The Central Records computer system, as administered by Information Systems Division, City of Springfield requires that passwords are changed every 45 days automatically or the account

3 Section III heading revised, per Policy Change Order 17-014.
4 Section 1.1 revised, unnecessary words removed, per Policy Change Order 17-014.
5 Section 1.1.1 revised, RSMo reference updated, per Policy Change Order 17-014.

holder is locked out of the network. Employees shall change passwords prior to being locked out.

2.1.1(a) All access is controlled by account and password security.

2.1.1(b) Only Information Systems Division staff has information related to access violations. Such violations are handled through administrative and/or criminal investigation, as appropriate.

2.1.2 The assigned system administrator for the automated records management system shall annually request a list of all police network account holders from the Information Systems Division, City of Springfield. (CALEA 82.1.6(d)) [6]

2.1.2(a) Upon receiving that list, the automated records management administrator shall verify all account entries as current employees with authorized access and make any necessary changes to RMS accounts in addition to advising Information Systems in writing, of any additions or deletions from the list.

2.2 Has authorization, through the bureau commander, to request access to employee files from Information System Division, in the absence of the employee, that require an immediate response or action. This may occur when the employee's supervisor has knowledge of an important assignment being handled by the employee and circumstances require immediate file access.

2.3 Provides Information System Division and Communications Department employees access to workstations for routine maintenance, loading software or reconfiguring.

2.3.1 Should unauthorized hardware or software be located on employer provided equipment, Information System Division or Communications Department employees have the authority to remove such equipment or software after notification of the supervisor of that workstation.

2.3.1(a) Unauthorized hardware or software includes all equipment or programs not purchased or licensed by the city.

2.3.2 Discovery of unauthorized hardware or software at a workstation shall be documented by the supervisor and sent to the City's Network Administrator.

6 Section 2.1.2 revised, *5th Edition* removed from CALEA standard reference, per Policy Change Order 17-014.

2.4 Makes request to the Information System Division Network Operations Center (NOC) or Communications Department for deletion of accounts as needed due to employee transfer, termination, etc.

2.5 Coordinates the purchase and installation of new or revised hardware through the Information System Division Support Center to assure the continued preservation of the system's integrity.

2.6 Coordinates the movement, disconnection or disassembly of computer components (computers, printers, modems, etc.) through the Information System Division Support Center.

2.7 Reviews files relevant to employee assignments that need revision or purging. Authorizes the purging of files in coordination with other department supervisors (when files are used by other department employees), the Information System Division, and Communications Department.

2.8 The City of Springfield will only authorize the use of a personally owned laptop computer for City business in special cases approved by the Network Administrator.

2.8.1 Ensures employees authorized to use a personally owned laptop for City business read and sign a waiver regarding their and the City's obligations.

2.8.1(a) A waiver shall be signed for each laptop authorized.

2.8.2 Confirms that backup disks of City business on personally owned laptops are current and accessible at all times.

2.9 The Information Systems Support Center will work with the Investigations and Support Services Bureau in maintaining an inventory of all Department computer hardware and software.

2.10 Information Systems Division, City of Springfield complies with internal procedures for maintenance of City network computer files including daily system backups and archiving. (CALEA 82.1.6(a)) [7]

3 EMPLOYEE RESPONSIBILITY

3.1 Toward local and non-local networks.

3.1.1 Be knowledgeable of the policy and operations manuals related to all computer systems used.

3.1.2 Be knowledgeable of other computer related policies, such as SOG 308.2 – Electronic Mail. [8]

3.2 Internet activity.

3.2.1 Use of the Internet shall be for city business only.

7 Section 2.10 revised, *5th Edition* removed from CALEA standard reference, per Policy Change Order 17-014.

8 Section 3.1.2 revised, punctuation change for consistency, per Policy Change Order 17-014.

3.2.2 Discretion should be used when downloading of files from the Internet. A number of sites available on the Internet such as Bulletin Boards may contain computer viruses.

3.2.2(a) All downloading of files from the Internet should be to the user's local hard drive (C: Drive) or portable/removable storage device.

3.2.2(b) Downloaded files are to be scanned for computer viruses prior to transferring to any network.

3.2.2(c) Should viruses be detected the Information Systems Division Support Center should be notified immediately.

3.3 Before using a personally owned laptop computer, employees shall secure authorization from the City's Network Administrator and sign a waiver.

3.3.1 Adhere to all laws, policies and merit rules that apply to use of personally owned laptops when used for City business.

3.3.2 Do not store any information related to City business on the machine.

3.4 Exercise caution to protect the system's integrity.

3.4.1 Exercise a high level of security with remote accounts (remote dial-up access to City and Police Network) and direct access accounts or from a stationary workstation within the department.

3.4.2 Upon activating the account the employee selects a unique password to gain future access to the account, per the systems policy.

3.4.2(a) Passwords do not entitle the employee to a sense of privacy. The department may engage in monitoring of electronic files created by employees for valid purposes, including employee supervision. This applies to personally owned computers when used for City business.

3.4.3 Employees shall not disclose their password to others or attempt to obtain other persons' passwords.

3.4.4 Log out of the system when absent from the workstation so as not to create a security hazard.

3.4.5 Routinely reviews files for purging of old or unneeded files they created for their use only.

3.5 Exercises caution to protect the system's physical well being.

3.5.1 Installing or deleting of software on employer owned equipment is prohibited unless directed by the Information Systems Division Support Center.

3.5.2 Movement, disconnecting or disassembling of computer components (computer, printer, modem, etc.) from workstations is prohibited

unless directed by the supervisor through the Information System Division Support Center.

3.5.3 Coordinate through the supervisor and report to the Information System Division Support Center or Communications Department all equipment that is malfunctioning.

3.5.4 Maintain workstation clean and free of dust and dirt.

3.5.5 Keep food, liquid, and other harmful articles away from computer workstations.

3.5.6 Exercise the same high level of physical security for laptops and other portable computer components as with other department computer equipment.

4 SOFTWARE USAGE

4.1 Computer software generally is a licensed product. The city purchases the right to use a computer program on a specified number of workstations. The department respects all computer software copyrights and adheres to the terms of software licenses.

4.1.1 Employees shall not duplicate any licensed software obtained for the department's use.

4.1.2 Shareware software is also copyrighted material that is distributed free for a trial period. Should the department or employee have a qualified use of a shareware program those programs shall also be licensed.

4.1.3 Employees personally owned/licensed software shall not be installed on city owned equipment.

5 RESTRICTIONS

5.1 Use of any PC or workstation for any purpose which violates any federal, state, or local laws is prohibited

5.2 Personal use of Police Department network computer workstations is discouraged. However, there may be legitimate uses for the network involving work which is reasonably relevant to the organizational mission, and is therefore authorized.

5.2.1 Personal use of MULES, NCIC, intelligence, or local file databases is strictly prohibited. Unauthorized use of such databases will be met with disciplinary action and, in some cases, may result in criminal prosecution.

5.3 Use of any PC or workstation for commercial purposes, for financial, or for material gain while on or off duty is prohibited.

5.4 Sending harassing, intimidating, abusive or offensive material to or about others is prohibited.

5.5 Using another person's identity and another person's password is prohibited.

5.6 Employees shall not add, remove, or reconfigure employer owned computer components without approval of the supervisor through the Information System Division Support Center. This includes hardware and software.

5.7 Employees experiencing system network problems shall not shut off the PC or workstation until the appropriate system administrator (IS Support Center or ECD) has been contacted.

5.8 The use of Power on Passwords/Application Passwords shall only be used with supervisory permission and be on file with supervisors and accessible by system administrator representatives.

5.9 Unplugging workstations from surge protectors is prohibited.

5.10 No software shall be added, deleted or in any way modified in the CAD terminals. All such requests or needs shall be routed to the CAD System Administrator in the Emergency Communications Department.

IV Attachments