

SPRINGFIELD POLICE DEPARTMENT

Standard Operating Guideline

Effective Date: 04/04/2017	Supersedes Policy Dated: 11/30/2012	Rescinds:	SOG Number: 308.2
Accreditation Index:			
Part Title: Support Services	Chapter Title: Information Systems Management ¹		
Chief of Police:			

Electronic Mail

I Policy

The Springfield Police Department continually strives to improve the efficiency of information flow with electronic communication services. Employees should utilize local and wide area computer networks, voice mail, facsimile transmission, electronic mail (E-mail), the Internet and the Intranet. Use of e-mail should be consistent with common sense, common decency, and civility applied to the electronic documentation environment.

II Definitions

E-Mail – Computerized transmission of written correspondence.

Encryption – Encoded electronic message.

File Server – Network device which manages access and storage of network files.

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

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.

¹ Chapter Title revised, typographical correction, per Policy Change Order 17-015.

SOG 308.2

Electronic Mail

Effective Date: 04/04/2017

III Procedure ²

1 LEGAL OBLIGATIONS

- 1.1 Use of e-mail and City telephones is subject to all federal, state, and local law, including: ³
 - 1.1.1 RSMo 569.095 - 569.099 concerning computer crime. ⁴
 - 1.1.2 RSMo 573.010 - 573.065 concerning pornography and related offenses.
 - 1.1.3 The Federal Communications Decency Act of 1996.
 - 1.1.4 The Missouri Sunshine Law, RSMo 610.029.
- 1.2 Attachment of copyrighted materials to e-mail or inclusion of copyrighted material in e-mail is strictly prohibited under federal statutes.

2 CITY DEPARTMENT OF INFORMATION SYSTEMS

- 2.1 The computer systems administrator is responsible for activating the employee account after the employee has received training in the use of e-mail.
- 2.2 The Department of Information Systems (IS) is responsible for technical support, maintenance, routine file back-ups, trouble-shooting hardware and software problems, preventing unauthorized access and system misuse.
- 2.3 IS will monitor account activity as necessary. They will assist supervisors in retrieving department related e-mail messages in the absence of employees.
 - 2.3.1 This may occur when the employee's supervisor has knowledge of an important e-mail message in the employee's account, and the employee is absent, and there is a need to retrieve that message.

3 SUPERVISOR RESPONSIBILITY

- 3.1 Makes requests through the Department of Information Systems representative to the system administrator for employee e-mail accounts and purging of accounts.
- 3.2 Authorizes e-mail accounts as needed, subject to approval by the employee's Bureau Commander.
- 3.3 Verify employees receive proper training or instructions prior to using e-mail.
- 3.4 Retrieves and processes important e-mail or employee files in the absence of the employee that require immediate response.

2 Section III heading revised, per Policy Change Order 17-015.

3 Section 1.1 revised, unnecessary words removed, per Policy Change Order 17-015.

4 Section 1.1.1 revised, RSMo reference updated, per Policy Change Order 17-015.

SOG 308.2

Electronic Mail

Effective Date: 04/04/2017

3.4.1 This may occur when the employee's supervisor has knowledge of an important e-mail message in the employee's account and the employee is absent, and there is a need to retrieve that message.

3.5 Supervisors, with Department Head approval, have the authority to inspect the contents of any equipment, files, calendars, or electronic mail in the normal course of their supervisory responsibilities.

3.5.1 A request for such activity should be directed to the Director of Information Systems.

4 EMPLOYEE RESPONSIBILITY

4.1 Exercise caution to protect the system.

4.1.1 Upon activating the account the employee selects a unique password to gain future access to the account.

4.1.1(a) Employees should not disclose their password to others or attempt to obtain other persons' passwords.

4.1.1(b) Passwords do not entitle the employee to a sense of privacy. The department may engage in monitoring of electronic mail messages or other electronic files created by employees for valid purposes, including employee supervision.

4.1.2 Log out of the system when absent from the workstation or utilize a screen saver password for temporary absences.

4.1.3 Employees should not open suspicious e-mails or open attachments to e-mails from unfamiliar addresses without first contacting the HELP DESK in IS.

4.1.4 Outbreaks of any virus, worm, or related malfunctions should be reported immediately to the HELP DESK.

4.2 Prompt response to e-mail is a matter of common courtesy. E-mail should be responded to just as you would respond to telephone messages, voice mail, and other correspondence.

4.2.1 If an employee has an e-mail account, they are responsible for checking their e-mail account at least once during the workday.

5 RESTRICTIONS

5.1 The use of E-mail for any purpose which violates any federal, state, or local laws is prohibited.

5.2 The use of E-mail for commercial purposes is prohibited.

5.3 Misrepresenting your identity or affiliation in e-mail communications is prohibited.

SOG 308.2

Electronic Mail

Effective Date: 04/04/2017

- 5.4 Sending harassing, intimidating, abusive or offensive material to or about others is prohibited.
- 5.5 Intercepting, disrupting, or altering electronic communications packets is prohibited.
- 5.6 The use of someone's identity and password is prohibited.
- 5.7 Causing congestion on the network by such things as creating "chain letters" or broadcasting inappropriate messages to lists or individuals is prohibited.
- 5.8 Employees may utilize City computer workstations for the transmission and reception of personal e-mails subject to the following terms:
 - 5.8.1 Personal use shall be reasonable and not interfere with the work performance of the employee;
 - 5.8.2 Personal e-mail use is expected to conform to those other restrictions for e-mail use presented in this section;
 - 5.8.3 Employees enjoy no legal protection or privacy interest in e-mail content sent or received in the City system.

6 VOICE MAIL SYSTEMS

- 6.1 Each employee is provided with either a telephone extension with voice-mail or a voice-mail box through the Meridian Mail system.
- 6.2 Each employee is responsible for:
 - 6.2.1 Attaching a professional greeting which includes:
 - 6.2.1(a) Working hours or, in the case of an officer assigned to the field, an explanation that working hours vary greatly.
 - 6.2.1(b) Reassurance that you will check your mail box as soon as possible.
 - 6.2.1(c) In case of emergency, referral to 911.
 - 6.2.1(d) Other non-emergency police service or immediate information, referral to TELCOM (1810).
 - 6.2.2 Checking messages and returning calls each working day.
- 6.3 If a return call is deemed to be inappropriate (such as an irate citizen), contact your supervisor for guidance/assistance.

IV Attachments