GENERAL ORDER 13.3.7

Use of Computer, Office, and Special Communications Equipment

GENERAL ORDER CROSS-REFERENCE: None.

SUMMARY

This policy establishes rules governing employee use of City provided Electronic Mail, Internet, Intranet, city computers, office and special communications equipment (i.e. SunGard, EIS, ReportBeam). Computer use must be consistent with CJIS Security Policy, Oregon Public Records Law, the state ethics statutes, and federal copyright and licensing laws. The City reserves the right to review any information, files, communications or programs sent, stored, received or loaded on its computer systems.

DISCUSSION

ORS 244.040: "Code of ethics; prohibited actions; honoraria. The following actions are prohibited regardless of whether actual conflicts of interest or potential conflicts of interest are announced or disclosed pursuant to ORS 244.120(1)(a). No public official shall use or attempt to use official position or office to obtain financial gain or avoidance of financial detriment that would not otherwise be available but for the public official's holding of the official position or office, other than official salary, honoraria, except as prohibited in paragraphs (b) and (c) of this subsection, reimbursement of expenses or an unsolicited award for professional achievement for the public official or the public official's relative, or for any business with which the public official or a relative of the public official is associated."

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB).

The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

The Department will abide by the CJIS Security Policy as well as internal CJIS policies and practice.

This General Order is not intended to supersede City Policy or CJIS Security Policy but rather to enhance the policy.

POLICY

I

DEFINITIONS

Computer System means, but is not limited to, a set of related, connected or unconnected, computer equipment, devices and software.

Data means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer, or in transit, or presented on a display device. Data includes, but is not limited to, computer or human readable forms of numbers, text, stored voice, graphics and images (system management information, configuration files, etc.).

II

Computers; office machines; and specialized communications equipment such as cellular telephones, FAX machines, modems and pagers are provided to Department employees for official use only. Personal use of this equipment may be granted by supervisors where such use is in the best interest of the Department**.** Personal use of City owned FAX machines is strictly prohibited.

Computers containing CJI data are required to be in a physically secured location.

Messages and data created, sent, stored or retrieved via Department owned equipment including but not limited to computers, telephones, voice mail, E-mail, pagers, modems, radios and FAX machines may be reviewed and audited by authorized City personnel. Such messages and data are City property. When creating, sending, storing or retrieving such messages and data, employees should not expect confidentiality and have no right to privacy from the City.

Employees shall receive appropriate training before using any of the above-named equipment.

III

The use of City-provided land line telephones will generally be limited to work-related duties. Exceptions to this include using a City land line telephone to talk to family members, make medical appointments, schedule service technicians, confer with a child's school or take

care of any of a variety of other matters which can only be accomplished during "regular" working hours. Personal telephone calls made during working hours from public employers' telephones should be brief and infrequent. Personal long distance calls may not be made on City telephones, even if the employee reimburses the City for the cost of such calls. If it becomes necessary for a City employee to make personal long distance calls while at work, such calls must be made with the employee's personal calling card or from a pay phone.

IV

No employee shall knowingly access, attempt to access, or use, or attempt to use, any computer, computer system, computer network, any part thereof, computer software, or data without authorization, in an unauthorized manner, or for unauthorized purposes.

No employee shall alter, damage or destroy any computer, computer system, computer network, or any computer software, documentation, or data contained in such computer, computer system or computer network without authorization.

The City of Springfield licenses the use of computer software from a variety of outside companies. The City of Springfield does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it. City of Springfield employees shall use the software only in accordance with the license agreements. The City of Springfield does not condone the illegal duplication of software.

City of Springfield employees shall load software on City computer systems only in accordance with the City software registration process.

Passwords and other security devices shall be kept confidential and not shared with other users.

Data generated and/or residing on City Computer equipment or generated by City employees using City computers for City Program activities are City property. This includes minor and incidental personal use.

Internet, City Network, and E-mail services as well as City Computers and software are provided by the City for employees' business use. Minor and incidental personal use which does not interfere with City business is permitted unless this type of use is denied by the employee's supervisor. Personal use must be infrequent and must:

- Not involve any prohibited activity;
- Not interfere with the productivity of the employee or of co-workers;
- Not consume system resources or storage capacity on an ongoing basis;
- Not involve large file transfers or otherwise deplete system resources available for business purposes;
- Not involve down loading, installing, or running software programs not acquired and installed by the Information Technology department;
- Not occur during normal working hours. Minor and incidental personal use is only permitted before or after normal working hours, or during breaks.

Prohibited Activities

Employees are strictly prohibited from using City E-Mail, Internet, City Network, Specialized Communications Equipment and City Computer services in connection with, by way of illustration but not of limitation, any of the following activities:

- In violation of current CJIS Security Policy, which can be found on the Oregon State Police LEDS website.
- Using City computers or any City-provided computer service for personal financial gain (such use is clearly prohibited by ORS 244.040(1)(a));
- Using City computers or any City-provided computer service to avoid financial detriment (such use is clearly prohibited by ORS 244.040(1)(a));
- Using City computers or any City-provided computer service for the financial benefit of a business or to avoid financial detriment to a business in which the employee or a relative of the employee has an interest;
- Use of personally owned devices on the City Network to include personally-owned thumb drives, DCs, mobile devices, tablets on WiFi, etc. Personally owned devices should not store City data, State data, or FBI CJI.
- Engaging in illegal, fraudulent, or malicious conduct;
- Working on behalf of organizations without any professional or business affiliation with the City; or working on behalf of organizations with such affiliation but outside of the specific City business with them;
- Sending, receiving, or storing offensive, pornographic, obscene, or defamatory material;
- Soliciting or supporting political or religious causes or beliefs;
- Annoying or harassing other individuals, including any prohibited form of harassment;
- Downloading or running materials including screen savers, music or streaming video off the web without previous authorization from their department director;
- Downloading software off the web without previous authorization from the Information Technology Department;
- Obtaining unauthorized access to any computer system;
- Using another individual's account or identity without explicit authorization of the individual, unless this is approved by the director of IT or the City Manager;
- Distributing or storing chain letters, jokes, solicitations, junk mail, offers to buy or sell goods, or other non-business material of a trivial or frivolous nature;
- Giving non-City employees or other users not authorized by a department director access to the Internet, City Network, E-mail, or computers;
- Purchasing, acquiring or installing software or hardware without previous authorization from the Information Technology Department.
- Streaming music, videos, movies or television programs

Employees violating this policy are subject to discipline, up to and including termination of employment. Furthermore, employees using the City's computer system for defamatory, illegal, or fraudulent purposes also may be subject to civil liability and criminal prosecution. Any employee who knows or should have known of a violation of this policy shall inform a supervisor or command officer immediately.

Failure to abide by the requirements of this personnel rule may subject the employee to disciplinary action up to and including termination. It is noted that employees are also subject to the provisions of ORS 164.377, Computer Crime. Under U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000, per occurrence, and criminal penalties including fines and imprisonment**.**

V

Damage to or failure of equipment shall be promptly reported to a supervisor.

Richard L. Lewis
Chief of Police