DEPARTMENT GENERAL ORDER 07-60

OFFICE of the CHIEF OF POLICE DATE: March 23, 2007
REPLACES: General Order 00-27
SOP 401.02.00

COMPUTER/SOFTWARE USAGE AND SECURITY

I. PURPOSE.

Increased departmental reliance upon personal and server computer systems to manage data and improve productivity, necessitates that the integrity of the systems be protected from unauthorized access. To accomplish this task, appropriate security measures in the form of passwords, passphrases, access codes, electronic audits, and back-up files will be utilized under the direction and control of Management Information Services.

II. DEFINITIONS.

Audit - An official examination and verification of records and/or data.

Computer Software - Written programs, to include general subroutines, that may be inserted in a computer system, or downloaded from same.

Password - An arbitrary and/or randomly selected word or collection of symbols used to limit access to computer systems to authorized personnel only.

III. GENERAL.

The protection of the department's various computer systems, and the data contained within those systems, is essential to the effective operations of the Police Department. To ensure the appropriate level of security is maintained, the following protective measures and procedures have been developed by the MIS staff.

1). Malware protection programs (anti-virus, anti-spyware, and anti-spam) have be installed on each computer and/or server to secure same from electronic corruption, and the loss of both processed data and damage to internal programming.

2). Multiple levels of "firewalls" or programmed security systems have been implemented to prevent unauthorized access to department computer data.

3). Procedures have been developed to control the unauthorized introduction or downloading of software programs to or from department computer systems.

4). Procedures have been developed to preserve electronic data via routine back-up operations and off-site storage.

IV. ANNUAL AUDIT OF COMPUTER SYSTEMS.

Department personnel who are authorized to access one or more of the department's computer systems shall each possess an individual password or passphrase to enable them to do so. Employees shall select their own individual passwords/passphrases which they will then utilize for approximately one month. Should an individual attempt to access the computer system without a proper password, or inadvertently use the wrong password, internal security provisions will activate after ten failed attempts, and the computer system will not only lock up but create an electronic log to document the incident.

Management Information Services shall conduct an annual audit regarding the assignment and/or changing of passwords and access codes to both individual personal computers and the department's server systems. However, in the case of the latter, the audit will be conducted in conjunction with employees assigned to the Administrative Division. Revisions in access codes, etc. shall be recorded by MIS personnel and maintained in a secure location.

In the event a department employee should retire or resign, that individual shall be deleted as an approved user on the system network as soon as practical.

V. COMPUTER SOFTWARE USAGE.

Each personal computer software program purchased by the City of Clayton is to be used according to the license agreement with the company that developed the product. City-owned computers and software are to be used for City business purposes, and only software provided by the City of Clayton shall be used on City-owned property.

City employees and affiliates who use computer software have a responsibility to ensure that no unauthorized copies of such software are created or used. This includes taking unauthorized software copies for home use or providing them to family members or acquaintances. Copying software without permission is unethical and illegal. As such, same is prohibited by the City and/or the software vendors utilized by the City.

The purpose of such restrictions is as follows:

1). To avoid criminal and civil penalties against the City and its employees.

2). To protect the City from civil litigation by software publishers for unauthorized copying.

3). To encourage publishers to provide the City with the most current and efficient software products.

4). To prevent damage to City-owned computer systems/equipment from viruses transmitted from non-City provided software.

As such, each City employee and affiliate who uses personal computer software shall:

1). Use only software provided or authorized by MIS on City-owned personal computers.

2). Obtain authorization from MIS before duplicating any software program.

3). Safeguard copies of software provided by the City from unauthorized use and duplication.

4). Prevent contamination of City-owned computer systems by computer viruses.

Management Information Services is responsible for the general administration of the City's software usage policy. Reports of unauthorized software or copying, or such other actions which may endanger the integrity of the City's computer system shall be reported to the Director of MIS. To assist in the enforcement of this policy, the following procedures shall be followed:

1). The supervisor of each work unit will be responsible for ensuring that subordinate employees who have access to City-owned computers and associated software adhere to this policy.

2). On a random basis, personnel assigned to Management Information Services will conduct audits of software residing on city-owned personal computers to ensure compliance with established policy.

The duplication or installation of software, which has not been approved or authorized by the City, may result in disciplinary action being initiated against the employee involved, up to and including dismissal. In addition, such actions may subject the City, and the employee or affiliate, to criminal or civil sanctions under the copyright laws of the United States.

VI. FILE STORAGE AND BACK-UP.

The Management Information Systems Department shall be responsible to back-up central records computer files on a daily basis. Each back-up process shall be automatically recorded on a computerized log, and the computer tapes generated as a result of the procedure shall be appropriately labeled and stored in a secure location. Back-up tapes shall be stored both on and off-site, and will comply with all State of Missouri record retention laws. Access to the off-site storage area will be limited to MIS personnel.

Computer data tapes shall be recycled as necessary. However, once a tape has reached the end of its useful life, same will be erased and then dismantled into its component parts to prevent unauthorized access to the data contained on same.

BY ORDER OF:

THOMAS J. BYRNE
Chief of Police

TJB:dld
CALEA Reference: 82.1.6