

754.8 SUBJECT: PERSONAL COMPUTER SOFTWARE AND DATA POLICIES

:1 .OBJECTIVE:

To set forth the policies with regard to Personal Computer Use, Hardware and Software.

:2.. AUTHORITY:

This procedure amended by City Council June 23, 2008.

:3. .DIRECTION:

Personal Computer Users, Division Managers, Office Heads, Department Directors.

:4.. FUNCTIONS:

A. Personal Computer Software

- 1 *Personal Software* - Software owned by individual employees will not be loaded or used on City-owned computers. Such software is not covered by the City's insurance policy, and is an unacceptable risk to the City of copyright infringement, public record violation and software virus infection.
2. *Copyrighted Software* - Only copyrighted software properly licensed will be utilized in City-owned equipment. The Technology Management Division (TM) will not provide help, assistance, or guidance to any person attempting to install, use, or maintain an illegal copy of a software product.
3. *Public Domain Software* - Public Domain software is defined as any non-copyrighted software obtained at little or no cost from public bulletin boards, computer clubs, professional organizations, or other public or non-profit entities. Public Domain software will not be used on City-owned computer equipment without prior authorization from TM. Authorization may be obtained from the Systems & Networks Program of TM as follows:
 - a. A justification specifically stating how the software will be used and that it is required by the user department to conduct City business. This justification must be signed by the Department Director/Office Head/Division Manager.
 - b. Software will be forwarded with the justification to the Network Support Manager, who will make every effort to assure the software is clean of virus and operates as it should. However, not all viruses can be detected and TM cannot guarantee or assure the software operates properly.
 - c. The Network Support Manager will return the clean software with an authorization letter to the user. The letter should be retained as proof of authorization and legality for audit purposes.

4. *No Cost Software* - Software given to the City by a vendor, or provided through another government agency may be used on City-owned equipment provided authorization has been obtained from TM. Authorization for use of this software may be obtained in the same manner as Public Domain software described above.
5. *Responsibilities and Auditing* - TM personnel will report any unauthorized software found on City-owned computers to the Department Director/Office Head and the Chief Information Officer. Program managers are responsible for assuring only authorized, legal software is used to conduct City business in their programs. Periodically, personal computers will be audited for compliance with this policy. Employees found with illegal software may be subject to disciplinary action. Unauthorized software will be confiscated and destroyed to protect the City from claims of software piracy or any other such claims.

B. Personal Computer - Data

The transfer of data from or to a City-owned computer from a non-City owned computer significantly increases the risk of infection by computer viruses. Prior to attempting data transfer , the following procedures must be followed:

1. *One-Time Transfers* - Media containing the data should be brought to Systems & Networks, where it will be checked for viruses before it is loaded to any City-owned computer.
2. *Recurring Transfers* - Data may be transferred from a non-City owned computer to a City-owned computer if it can be reasonably determined that the risk of infection on the non-City owned computer is low. Prior to transferring data on a recurring basis, employees should contact the Technology Management Division for free anti-virus protection and instruction on risk reducing procedures.
3. *Confidential Data* - Data kept on City-owned Computing devices should be protected with secure passwords and, where, practical encryption technologies used to protect the integrity and privacy of the data. Missing or stolen hardware containing City data should immediately be reported to the Security Officers in the TM Division along with the relevant Program Managers. In cases where it is possible and practical the data on the device may be deleted and the device immobilized remotely. Copies of software and/or data made for backup, archival or distribution purposes should be reasonably protected to ensure the software or data is not used for illegal, illicit or unauthorized purposes.

C. Continuity of Operation

Immediate supervisors are responsible for ensuring continuity of operations with regard to computer equipment within their program. This means ensuring that necessary backups of software and data, located on local personal computers, is taken on a timely basis and stored with proper protection.

D. Use of City-owned Computers

Employees are prohibited from using City-owned computers for any jobs outside the scope of their employment with the City, with the following exceptions:

1. To generate material in support of educational pursuits under the City's Educational Reimbursement Policy.
2. To generate material for special projects when authorized by the Office Head, Department Director or Division Manager.

E. Monitoring and Misuse of City-owned Computers

Personal computers that are the property of the City and any contents thereof, including email, are subject to monitoring and access by the City at any time with or without employee consent. It is strictly prohibited to use a City computer to seek, send or store material that;

1. is sexually explicit, pornographic, or obscene;
2. can be construed to be harassing or disparaging of others based on their sex, race, sexual orientation, national origin or religious or political beliefs;
3. has the potential to cause the City public harm or disrepute; or
4. violates any law or City policy

:5. FORMS:
None.

:6. COMMITTEE RESPONSIBILITIES:
None.

:7.. REFERENCE:
Procedure adopted by City Council December 18, 1989, Item 16A-47; amended July 16, 1990, Item 3A-9; amended and renumbered from 753.2 on December 9, 1991, Item 6/NN; amended November 9, 1992, Item 6J; amended April 19, 1993, Item VV; amended March 20, 1995, Item SS; amended August 31, 1998, Item 3; amended April 3, 2000, Item 2PPP; amended September 15, 2003; amended June 23, 2008.

:8. EFFECTIVE DATE:
This procedure effective June 23, 2008.