3-05/160.00 - Regulations for Installing Software on Computers at Sheriff's Department Facilities

Unauthorized copying, installation, and/or use of licensed software is prohibited by federal law. To ensure that members do not place themselves or the Department in jeopardy of violating copyright infringement laws, Unit Commanders are responsible for the management of software utilized by personnel under their command at Department facilities. Required actions by unit commanders include the following:

- All software programs, whether purchased, public domain, free or demonstration/evaluation type license, shall be documented and maintained in a unit systems library. The library must be supervised by a staff member specifically designated by the unit commander. Selection of staff for this function is not restricted by rank or title and should be the most qualified person(s);
- Software provided on removable media (i.e., disk, CD-Rom, removable hard disk) must be kept in a locked cabinet. If the software is maintained in an electronic file (i.e., accessible hard disk or network), strict access controls within the computer system must be in place. Procedures to record the receipt, removal, transfer, and/or disposal (returned/destroyed) of software shall be maintained;
- A request for evaluation of a software program at a unit or facility can only be authorized by the unit commander, who must determine the need for retention and ensure the safe return of the product. When software is received at a unit, standardized logs and evaluation forms must be used to track the testing and review of the software. The evaluation software must be tracked through the testing period and properly disposed of at the end of the evaluation period. Department forms for this process are available on request from the Data Systems Bureau;
- Proper procedures for avoiding copyright violations must be reinforced through training at each unit. Recurrent briefings, unit meetings orientation of new employees, and unit optional training methods must be utilized and documented by the unit commander to emphasize the Department's position;
- Access to all computer equipment where software can be copied to removable media in violation of license agreements must be restricted to personnel authorized by the unit commander. In situations where computers are networked, or individual computers contain critical software or data, proper password security must be in place;
- Software licensed by one unit and provided to and utilized by Department personnel of another unit on controlled computers, requires dual responsibility. The control of the licenses is the responsibility of the providing unit's commander. Ensuring that the license agreement is not violated by unauthorized copying, installation and/or use at the specific unit where it is installed is the responsibility of that unit commander;
- Software utilized by on-duty Departmental personnel on their personally owned computers located on county property must be licensed software; and
- Any computer equipment located at any off-site facility controlled by the Department is subject to the same rules as enumerated in this directive.

Inspections to insure compliance with this policy shall be accomplished in the following methods:

- Unit commander inspections;
- Random inspections by Inspectional Services Unit with technical assistance from the Data Systems Bureau; and
- Unannounced inspections by the chief administrative officer's staff.