3-07/210.30 - Computer Software and Files

Data Systems Bureau is responsible for selecting the standard desktop software suite for all Department computers and for administration of the software on computers connected to the Sheriff's Data Network (see section 3-07/230.00). All authorized persons shall use the selected desktop suite unless critical functionality is not available through the suite.

Authorized persons are required to keep the personal information section (properties) of the e-mail address book up-to-date. This includes title, work address, Unit of assignment, work location, work phone number, and fax number. Optional items include mobile phone number and pager number.

Security software, including but not limited to: anti-virus, anti-spam, and firewall solutions are a critical component of the multi-layered security structure protecting the Department. Given this criticality, Data Systems Bureau is responsible for selecting and configuring security software for all computers. Unless a specific exemption or modification is authorized by Data Systems Bureau, all authorized persons shall use the authorized software, use the authorized configuration, and ensure the software is kept current.

Authorized persons are prohibited from installing or maintaining unlicensed software on any Department computer. Authorized persons who wish to install licensed software on a Department computer must have authorization from their Unit Commander and Data Systems Bureau. The software installation and record of the installation will be the responsibility of Data Systems Bureau. Authorized persons are required to provide a copy of the software license to Data Systems Bureau prior to the installation.

Licensing agreements for some software applications permit Department members to install the software on their home computers. For a list of these applications, contact the Central Help Desk.

It is strongly recommended that users store files in their personal folder in the Unit file server. These files will be "backed up" daily to prevent loss of information. They cannot be accessed by other users and offer the highest degree of individual security. Any files stored on the local drive ("C" drive) of the computer are not secure against access by other users and will not be backed up to prevent loss of information. During routine maintenance, computers may be replaced or hard drives erased without notice to the user. Data contained on the local drive ("C"drive) of these machines/hard drives will be lost to the user.

The Department reserves the right to access and disclose the contents of employee-created electronic files and messages when a legitimate business need arises and without the permission of the employee.