FLORENCE POLICE DEPARTMENT
GENERAL ORDER

Subject: COMPUTER SOFTWARE POLICY	**Procedure:** General Order 4.4.4 CALEA 11.4.4	**Total Pages:** 2
Authorizing Signature: Original with Authorizing Signature on File	**Effective:** 01/01/2011	
	(X) **New** ( ) **Amended** ( ) **Rescinds**	

I. POLICY

It is the policy of this Department to conform to, abide by, and fully adopt all provisions within the City of Florence Information Technology Policy.

II. PURPOSE

This written order establishes guidelines regarding the use of computer workstations.

III. SCOPE

This written order is applicable to all personnel.

IV. RESPONSIBILITY

All Department personnel will comply with this directive.

V. ADOPTION

The Florence Police Department adopts the City of Florence Information Technology Policy. If any aspect of this directive is contrary to the Information Technology Policy, the Information Technology Policy has precedence.

VI. PASSWORDS

A. Employees shall not disclose their password to any person other than their immediate supervisor, the System Administrator, or the System Administrator's designee.

B. Generally, employees shall not use any computer workstation that is signed on under another employee's password without their prior knowledge.

C. Employees shall change their password any time that it is suspected or known that an unauthorized person or employee may have knowledge of it.

VII. SOFTWARE

Employees are prohibited from installing any software not provided by and properly licensed to the City of Florence. This includes but is not limited to Internet freeware. Employees may request permission from IT to install software they have purchased, provided that the original license will be on file at the Florence Police Department as long as the software is installed on the workstation.

VIII. HARDWARE

Employees are prohibited from installing any hardware, excluding speakers, not provided by the City of Florence. Requests for exceptions to this standard are to be addressed to IT personnel, and are to include approval by the Technical Services Division Commander.

IX. SECURITY

Workstations shall not be left signed on and unattended where they can be accessed by an unauthorized person. Employees should lock their workstation when they will leave it unattended. When employees utilize a shared workstation, such as in roll call, the employee vacating the workstation shall log off.

X. INTERNET AND INTRANET USE

Internet and Intranet access and email are provided for business purposes only and are routinely monitored. Access to sexually explicit or other sites that would be considered inappropriate for business is forbidden. Access to sexually explicit or other sites that would be considered inappropriate for business, but required for investigative purposes, must be approved by the employee's immediate supervisor. The supervisor approving access must coordinate access with IT personnel ahead of time, if possible.

XI. VIRUS PROTECTION

All employees must be aware of the possibility of introduction of viruses by utilizing computer data from unverifiable sources. If any employee has a question of whether or not a workstation, or other computer media has a virus, they should contact IT as soon as possible.