FLORENCE POLICE DEPARTMENT
GENERAL ORDER

Subject:	**Procedure:**	**Total Pages:**
COMPUTER USAGE REQUIREMENTS/MOBILE DATA ACCESS	General Order 19.3.7 CALEA 41.3.7	6
Authorizing Signature: Original with Authorizing Signature on File	**Effective:** 01/01/2011 (X) **New** ( ) **Amended** ( ) **Rescinds**	

I. POLICY

It is the policy of the Florence Police Department to provide appropriate protection and security to any and all information stored, processed, or input to a City owned or operated computer system that may be used by an employee of the City during the normal course of business.

II. PURPOSE

This written order establishes guidelines and regulations pertaining to computer workstation usage and security.

III. SCOPE

This written order is applicable to all personnel and applies to all information residing on computers and network systems owned by or administered by the City.

IV. RESPONSIBILITY

All personnel will be held responsible for compliance with the guidelines outlined in this directive.

V. ADOPTION

The Florence Police Department adopts and will adhere to the City of Florence Information Technology Policy Manual.

VI. COMPUTER WORKSTATIONS

Computer workstations are business tools, and are to be used for business purposes only. Each workstation is set up to provide the tools necessary to accomplish the tasks performed by the signed on employee. Any attempt to deliberately access any software not available to the signed on employee, or to access any restricted functions of the software provided is strictly prohibited.

A. PASSWORDS

1. Employees shall not disclose their password to any person other than the System Administrator or their designee.

2. In general, employees shall not use any computer workstation that is signed on under another employee's password; however it is

understood that a shared workstation such as the video computer in roll call prohibits 100% compliance with this standard.

3. Employees shall change their password any time that it is suspected or known that an unauthorized person may have knowledge of it. If you need assistance in changing your password, contact the System Administrator or your supervisor.

B. 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. Nor are employees authorized to manipulate or alter current software in a manner contrary to the provisions of this directive. Employees may request permission from the System Administrator to install software they have purchased, provided that the original license will be on file as long as the software is installed on the workstation. This provision applies to all department owned computer devices.

C. HARDWARE

Employees are prohibited from installing any hardware, excluding speakers or a flash drive, not provided by the City of Florence. Requests for exceptions to this standard are to be addressed to the System Administrator, and are to include approval by the appropriate Bureau Commander.

D. SECURITY

Workstations shall not be left signed on and unattended where they can be accessed by an unauthorized person. The workstation is to be locked when it is to be left unattended but the employee will return in a brief time. If the workstation cannot be locked by the utilization of a password, the workstation must be shut down to prevent unauthorized access. When employees utilize a shared workstation, the employee vacating the workstation shall log off or otherwise shut down the computer.

E. INTERNET AND INTRANET USE

Internet and Intranet access and e-mail are provided for business purposes only, and are routinely monitored. 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 maintain a log that records the date, time, site name, employee name and purpose of the access. This log must be maintained for a period of six months after the log entry date.

F. 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 disk, flash drive, or any other data source contains harmful data or a virus; they should contact the System Administrator.

VII. MOBILE DATA ACCESS

A. DEFINITIONS:

1. MOBILE DATA ACCESS EQUIPMENT – The laptop computers issued by the Department and used by personnel in field operations. This includes all accessories which enable the computer to be functional (i.e., computer, mounts, radios, antennas, air cards, and related cabling).

2. AUTOMATIC VEHICLE LOCATERS (AVL) – Automatic vehicle location equipment that uses Global Positioning Satellite signals to pinpoint the location of a vehicle, and relays that information to the Department's computer dispatching system.

B. PROCEDURES:

Departmental personnel will use their issued laptop each time they drive a vehicle with a laptop mount during their regular duty shift. This can be either their assigned vehicle or a spare vehicle that is similarly equipped.

1. DURATION: Officers will insure that they are properly logged on to the computer and mobile program is running prior to their regular duty shift. They will remain logged on to the computer until they finish their assigned duty and are at their residence or the Police Department where they park their vehicle when not on duty. (If technical problems occur that make it impossible to comply with this section, a supervisor will be immediately notified and corrective action will be taken to repair the equipment as soon as possible).

2. LOGGING ON TO MOBILE: Officers will log on to the mobile program when going in service for regular duty. They will remain logged in to mobile for the duration of their regular duty shift. Officers may utilize mobile when working secondary employment, but it is not required, as duty types vary on secondary employment.

3. MALFUNCTIONS: If the AVL is discovered as not functioning properly (vehicle is not appearing on the map) dispatch will be notified via the police radio. A supervisor will be notified and appropriate action will be taken to ensure that all of the installed equipment in functioning properly. If the supervisor cannot remedy the situation, the assigned officer will have the vehicle and laptop checked by the appropriate service personnel as soon as possible.

4. DISPATCH REQUIREMENTS: If a dispatcher becomes aware that a unit's AVL is not functioning properly, they will immediately notify a supervisor. The supervisor will then take appropriate action to have the situation remedied.

5. DISABLING AVL: At no time will an officer turn off, disable, tamper with, or in any way attempt to interfere with the proper operation of the AVL system.

6. MESSAGING CAPABILITIES: Electronic messages are not private or confidential. They may be monitored or retrieved by supervision, and are subject to court subpoena. The transmission of material that contains obscene or disparaging language or graphics is strictly prohibited. Officers may use messaging capabilities for departmental business only.

C. SYSTEM SECURITY:

To protect the integrity of the computer system, certain levels of security have been established. Employees are given a level of access into the computer system based on their job requirements. Employees shall not attempt to bypass, enhance or otherwise modify the level of security they have been given.

1. It shall be the responsibility of the employee to protect the security of their assigned equipment and their system password. At no time shall an employee use another employee's password to access the computer system.

2. Laptop computers shall be properly secured in a computer mount when used in a police vehicle. When the officer is not on duty, and the vehicle is parked at the Police Department or their residence, the computer will be properly secured in the mount or removed from the vehicle and taken to a secure location.

D. NCIC/ACJIS SECURITY:

The data accessed using the NCIC/ACJIS system must be protected to ensure correct, legal, and efficient dissemination and use. Officers must follow proper procedures to make the information secure from any unauthorized access or use.

1. The departmental laptop will have a link to the NCIC/ACJIS system. This system is password protected and allows officers to access classified records. The protection of passwords and the security of laptops are critical to prevent unauthorized access to NCIC/ACJIS data.

2. The NCIC/ACJIS system is to be used for law enforcement purposes only and is not to be used in violation of the 1972 Federal Privacy Act regarding the dissemination of criminal records to unauthorized personnel. Personnel operating laptop computers will

be held accountable for the protection of their respective passwords while accessing the system. Only authorized law enforcement personnel, while in the performance of their duties, are allowed access to the content(s) of any file retrievable through the computer. Whenever an officer accesses a file, the computer will create an audit trail of the transaction. This audit trail file can be accessed and can be used to determine which files were accessed, the time they were accessed and who accessed the file.

3. Any access to NCIC/ACJIS from a laptop computer is the responsibility of the officer whose password was used to log into the computer. Any officer, who allows unauthorized access, whether willfully or through negligence, is subject to disciplinary action and possible criminal prosecution. If an officer is using the laptop computer to access NCIC/ACJIS and a civilian or unauthorized person is in the vehicle, the officer must insure that the information on the computer screen is not visible to the unauthorized person. This may be accomplished by repositioning the computer screen or directing the unauthorized person to leave the immediate area of the vehicle.

4. Information from NCIC/ACJIS must be kept strictly confidential. Under no circumstances will any officer use another officer's password to gain access to the NCIC/ACJIS system. Under no circumstances will any officer use a laptop that is logged on by another officer to access NCIC/ACJIS.

E. NCIC/ACJIS HIT CONFIRMATION**:**

An NCIC/ACJIS hit advises the officer that a stolen report, missing person report, or arrest warrant has been filed. It also provides the date of theft, date missing, or date of warrant issue, which are matters to be considered by the receiving officer in arriving at an arrest decision. A hit is a fact which must be added to other facts by the officer in arriving at sufficient legal grounds for probable cause to arrest.

1. When an officer receives a positive response from NCIC/ACJIS and an individual is being detained, or a piece of property may be seized, an immediate confirmation with the agency that originated the record in the system is necessary to ensure the validity of the hit before an arrest or seizure may be made. To confirm a hit means to verify with the entering agency that the missing person report, theft, or warrant is still outstanding and that the person or property inquired upon is identical to the person or property listed in the wanted person, missing person, or stolen property record.

2. To initiate a hit confirmation, the officer must notify police dispatch and give the exact information that was entered on the laptop computer to generate the original hit. The dispatch

personnel will then resubmit the inquiry using the data supplied by the officer in the field. When the hit is received in dispatch, the operator will then contact the entering agency and verify the hit. Any further information received by Dispatch will be relayed to the officer in the field. The officer can then use the verified information to establish sufficient grounds for a probable cause to arrest and/or seize property.