	Administrative General Order	66 Departmental Computers	**PAGE 1 OF 6**
	City of Charleston Police Department Policy and Procedure Manual		EFFECTIVE DATE: **02/01/08**
			ORIGINATOR: **Strategic Analysis & Innovations**
			REVISED: **03/01/11**
	DISTRIBUTION: **ALL**	**CALEA:** 11.4.4; 82.1.6; 82.1.7	
BY THE AUTHORITY OF THE CHIEF OF POLICE:			

66.1 DEPARTMENTAL COMPUTERS

The purpose of this order is to establish departmental policy and procedure concerning the installation, de-installation, maintenance, service, and use of Charleston Police Department computer systems and their associated infrastructure. This includes, but is not limited to all desktop computers and laptop computers (also known as notebook pc's, portable pc's and the like; networks; peripherals; and software packages). These provisions are designed to ensure minimal problems with the computer equipment by verifying that all hardware and software installations are compatible with the existing and anticipated computer systems and that employees adhere to a uniform policy regarding operation and care of the system. Nothing in this order supersedes or amends the City of Charleston Computer Use Policy. All employees must comply with all City of Charleston policies and procedures.

66.2 DEFINITIONS (CALEA 11.4.4)

For purposes of this policy, the following definitions apply:

Assigned Component: A police department unit, section, division, or bureau that is assigned a department computer.

Assigned Employee: A police department employee who has been assigned a department computer.

Authorized User: An individual sanctioned by The Charleston Police Department, to utilize department computers. An individual may be sanctioned by the very nature of their training or assignment.

Computer Maintenance & Installations: Additions, modifications, or deletions of any software or hardware on a department computer, include opening the computer's external case.

Department Computer System: Any personal computer owned or maintained by the Charleston Police Department that includes all or some of the following:

1. Desktop: A computer and monitor that is stationary.
2. Laptop: A portable computer running a full commercial operating system capable of running off battery power alone.
3. Radio Modems
4. Modem Antenna
5. Other peripherals

Downloads: Copies of files obtained through removable media such as floppy disk, CD ROM disk, etc. or received from another computer.

Electronic Mail (Email): Electronic messages sent from one person, business, computer, program, or group via computer to another.

1. Departmental Email: Electronic massaging sent from one department to another department.
2. Internet Email: Electronic massaging sent from one person via Internet to another.
3. Attachments: Electronic files that can be sent with departmental or Internet email.

Log-in (Log-on) Access: Access to applications, files, peripherals, and department computers through the use of assigned user names and passwords for security purposes.

Log-off: When access is no longer needed, it removes access. A new login is required to regain access.

Network: A system of interconnected computers, which allows the sharing of files, software, printers, or peripheral equipment. Related items include:

1. Dial-up Access: The ability to access computers and files attached to a police LAN through software, security and a telephone modem, typically, from a remote location.
2. Internet: The global system of networked computers around the world.
3. Local Area Network (LAN): A group of computers connected together that have the ability to share files.
4. Modem: A device to send and receive electronic information documents, images, files) from a computer, usually through a telephone line.
5. Wireless: The ability to connect and send and or receive files wireless (i.e. - cellular phone system, cellular digital packet data, or other means).

Peripheral Equipment: Any equipment that is attached to a computer system (i.e., scanners, printers, cameras, CD-ROM drives, etc.).

Removable Media: Any device that stores information that can be removed from one computer and moved to another (i.e., floppy disks, CD-ROM disks, tape cassettes, etc.).

Software: The instruction set used to make the hardware (central processing chips, monitors, drives, etc.) perform tasks.

1. Application: Electronic code that performs a specific task on a computer (i.e.: Microsoft Word, MAJIC, Netscape, etc.).
2. Commercial Software: Software purchased to run on a particular system.
3. Freeware: Software freely obtained from public sources.
4. Police Software or Data: Software developed at or data collected within the police department (i.e. - Suspect File).
5. Shareware: Software obtained through public sources with normally limit features, periodic visual reminders to purchase or a time limit cutoff to prevent use without purchase.

Software Licensing: Software that is legally licensed and is installed so that it is in compliance with the associated license. Software purchased for one (1) computer often cannot be legally installed on any other computer because the original license allows only one (1) installation per license.

Unauthorized Software: Any software that has not been approved by the Administrative Services Bureau Commander or designated representative. This includes any software not required for job related duties.

Uploads: Copies of files sent to another computer.

66.3 GENERAL PROVISION

Installation / De-installation

To request the installation or de-installation of any software or hardware, the requesting personnel must submit to the Investigations/Support Bureau Commander, or designee, a written description of the items to be installed or removed. The Investigations/Support Bureau Commander or designee will review the request to establish:

1. Compatibility with the existing hardware;
2. Compatibility with the existing software;
3. Compliance with software licensing agreements; and/or
4. Proper registration.

If the request is approved, the Investigations/Support Bureau Commander, or designee, will schedule the installation or removal.

No software or hardware will be installed, upgraded, or removed from any department computer without the approval of the Investigations/Support Bureau Commander, or designee.

No personal computer or any other equipment may be connected to the department network, in any manner, without the approval of the Investigations/Support Bureau Commander, or designee. Only personnel authorized by the Investigations/Support Bureau Commander or designated representative will install approved equipment.

Software

No person will load software for personal use on any department computer. No person will use department hardware or software for personal use or personal gain. Supervisors or employees observing unauthorized software on departmental computers will report it to the Investigations/Support Bureau Commander, or designee, for review and will request removal of the software immediately. Employees using unauthorized software on department computers will be subject to disciplinary action. Unauthorized software is defined as, but not limited to, any software not issued or approved by the Charleston Police Department and the Charleston City Information Technology Division.

Restrictions

Employees with Internet access are to use such access for department business use only. Employees will log off the Internet after obtaining information. At no time will an employee maintain an Internet connection while not actively using the service unless directly connected to the Internet via a direct network connection. The Investigations/Support Bureau Commander, or designee, may monitor Internet activity by specific employee and specific Internet sites. Any employee who abuses Internet access privileges by accessing inappropriate sites, for other than department use, or using the Internet for other than work related activities may be subject to disciplinary action and/or the loss of Internet access privileges and/or the loss of the assigned computer(s).

The use of any department information or equipment for personal use is strictly prohibited. Computer access is made available for work related activity. The Investigations/Support Bureau Commander, or designee, will remove any unauthorized software found on police department computers.

Multiple users may share component computers as long as each user accesses information (email, NCIC, etc.) through their own assigned login. Laptop computers assigned to specific employees will remain with the component if the employee is transferred. Whenever an employee is transferred, that employee's component commander will ensure the assigned computer is returned to the Computer Services Director for reassignment within that component.

No employee will attempt to gain access to any area of the Charleston Police Department or Charleston Government computer system that they are not authorized to access. This includes, but is not limited to, other employee mailboxes or hard drives,

networked software programs, etc.

66.4 SPECIFIC PROVISIONS (CALEA 82.1.6 a, b)

Security and Storage

A specific employee, assigned a computer, will be responsible for the assigned computers physical security and for obtaining any required maintenance through the Director of Computer Services.

It will be the assigned employees responsibility to safeguard the computer using every precaution available (i.e. - locking their vehicle when left unattended, securing the computer in their residence or locking their office). To the extent possible, officers assigned computers utilized in the field will use every available precaution (locking equipment in vehicle trunk, etc.) when the equipment is not in their immediate possession or the vehicle is left unattended for extended periods.

It is the assigned employee's responsibility to ensure the security of the computer against unauthorized use. Employees will not give their passwords to any other persons to use nor will they leave the password in any discernible written form in or near their computer. They may be required to disclose this information to someone in their chain of command or support personnel for departmental business purposes. If the assigned employee leaves the computer unattended and are not in direct control of the system they are required to log off the system.

The Charleston City Information Technology Department will be responsible for loading and maintaining virus protection on all department personal computers and network drives. In addition, they will be responsible for providing information describing the use of utilities that safeguard the computer (virus scanning, file backup).

The Investigations/Support Bureau Commander, or designee, must be notified immediately if department computers or peripheral equipment are damaged or stolen or it is believed unauthorized access was attempted or gained.

Maintenance

Computer Services Director is responsible for all maintenance, support, and repair of department computers. Request for service will be routed through the Computer Services Director. Assigned employees will notify their immediate supervisor of any maintenance problems not resolved in a timely manner. This information will then be forwarded to the Computer Services Director.

In an effort to assist the Computer Services Director in resolving computer problems, the person reporting will make every effort to document the nature of the problem. The following items will be documented:

1. Date and time of occurrence;
2. Nature of occurrence (i.e. - computer out of memory, network services not available, or any message that appears in a dialog box showing an error);
3. Damages of any nature.
    a. Note that often damages can be minimized if the damage is reported promptly. Such is the fact in especially in cases of spilled coffee and like fluids into the computer. In cases of spilled fluids into the computer or the computer becoming wet from any source, the user is to immediately disconnect the power from the computer and remove the battery. Then, without delay, notify the on duty supervisor and the Computer Services Director. All other damages will also be reported immediately.

Inspections

Department computers are subject to line or staff inspections at any time.

Training

It will be the responsibility of the assigned employee to maintain National Crime Information Center (NCIC) certification. Failure to maintain this certification would place the employee in direct violation of this directive should he/her attempt to operate the assigned laptop computer to gain NCIC or SLED access.

It will be the responsibility of the Office of Professional Development and Training to design and administer additional computer training specific to the software available to the assigned employee.

Electronic Mail (Email) Procedures

Messages sent on the email system will be for department business purposes only.

An employee will not attempt to gain access to another employees' mailbox. However, a supervisor in the employees' chain of command will have the right to access an employees' mailbox for business purposes.

Employees will disclose to a supervisor in their chain of command any passwords and codes necessary to access the system upon request.

Emails with large or numerous electronic file attachments are discouraged. Employees with department email accounts and who are assigned a department computer are required to check for new messages each day they report to work. If an email account or computer access is no longer used (due to change in assignment, computer availability, etc.) the affected employee's immediate supervisor will notify the Computer Services Director to have the affected employee removed from the system.

Authorized personnel may retrieve email that is sent through the Charleston Police Department computer system at a later time, even though it may have been deleted from the assigned employee's computer. Email is not a protected form of communication and could be subject to a discovery motion in a criminal case, civil case, communication and could be subject to a discovery motion in a criminal case, civil case, or internal investigation. All email and car to car, dispatcher to car, and car to dispatcher messaging is logged and archived and may be reviewed by command staff or subpoenaed by a court of law.

Every electronic transmission will be considered in the public domain. Messages will be professional and courteous.

66.5 ANNUAL AUDIT (CALEA 82.1.6 d)

The security of records in the Police Department Computer System is vital. On an annual basis, there will be an audit of the central records computer system that will include at a minimum verification of all passwords, access codes, or access violations. The Charleston Police Department designated technology officer through the City of Charleston Chief Information Officer will complete this audit. The Chief of Police will forward a report of compliance with this procedure to the Administrative Services Officer of the Charleston Police Department for review.

66.6 OUTSIDE COMPUTER SOFTWARE AND DISCS

The introduction of outside software could result in virus infection of the entire system. Designated and authorized personnel of the City of Charleston must install all programs. All computer media will be inspected for virus infection before introduction in to any of the police department's computer system or associated equipment.

66.7 CENTRAL RECORDS COMPUTER FILES

Computer files must be backed-up according to the record retention laws or regulations of the State of South Carolina, the City of Charleston, and the Charleston Police Department Policies. The backup tapes, disc or drives must be stored in a secure facility or area, off-site from where the records are maintained or used. When the material is recycled, the method of destruction must ensure that the data is not retrievable for the discarded material. The designated technology officer for the Charleston Police Department will verify that this procedure is complied with and report compliance to the Administrative

Services Officer of the Charleston Police Department annually.

66.8 CRIMINAL HISTORY RECORDS (CALEA 82.1.7)

Any computer criminal history records must be secured and access or release of such record must conform to existing federal, state, and local laws and the policies and procedures of the Charleston Police Department and to the City of Charleston.