


# PINE BLUFF POLICE DEPARTMENT POLICY/PROCEDURES MANUAL

	<b>SUBJECT:</b>	<b>POLICY NUMBER</b> 118
	<b>Computer Security</b>	<b>ISSUE DATE</b> 02/19/2008
	<b>CHAPTER: ADMINISTRATION &amp; PERSONNEL</b>	<b>EFFECTIVE DATE</b> 02/19/2008
	<b>ISSUED By:</b> Chief of Police John Howell	<b>TOTAL PAGES</b> 13

## I. PURPOSE

The purpose of this policy is to provide instructions for members regarding Department computer systems, electronic mail (e-mail), and Internet usage.

All police computer systems, (including but not limited to the I.B.M. mainframe, Computer Aided Dispatch System, Mobile Data Computers and Terminals, Workstations, Laptops, Notebooks and the City-wide Net), hardware and software, are for the official use of Police Department employees and are intended to improve the efficiency and effectiveness of departmental operations.

Operation of all Department computer systems and programs must be in accordance with established security measures as outlined below and shall be limited by security access as determined by Administrative Services Division and training level. Records and information maintained by the Pine Bluff Police Department are for the exclusive use of departmental employees only and shall not be disseminated to persons who are not affiliated with a bona fide law enforcement agency or as directed by command supervisors. [CALEA 82.1.1d]

## II. DEFINITIONS

**BREACH** - A break in the system security that results in admittance of an unauthorized person or program to a Department computer system.

**ELECTRONIC MAIL (E-MAIL) MESSAGE** - Any document created or received on the Electronic Mail System. These documents include, but are not limited to, brief notes, announcements, memorandums, formal Department documents such as Department Memorandums or Job Vacancies, and any attachments to these messages, such as word processing or spread sheet documents.

**ELECTRONIC MAIL (E-MAIL) SYSTEM** - A computer application that is used to create, receive, transmit, store, and archive Electronic Mail Messages.

**FIREWALL** - A form of access-control technology that prevents unauthorized access to information resources by placing a barrier between an organization's network and an unsecured network.

**HARDWARE** - The physical computer system or any physical part or mechanism used as an integral or peripheral component of a computer system (e.g., a floppy or hard drive mechanism, memory modules, display monitor, interface card, etc.).

**INTRANET** - An Intranet uses Internet based technologies within an organization to facilitate communication and provide integrated access to information.

**INTERNET** - A worldwide network of computers linked together by various communication systems including local telephone services.

**NETWORK** - A system of computers, printers, and hard disks linked by direct connection, over telephone lines, or via other electronic transmission methods that allows shared access to all resources on the network.

**SOFTWARE** - The programming instructions and data the computer executes to perform tasks. The term "software" is often used to refer to the distribution media that contains it (e.g., floppy disk or CD-ROM), but more correctly refers to the actual instructions and data contained on whatever media is used.

1. **FREWARE SOFTWARE** – Software freely obtained from public sources.
2. **SHAREWARE SOFTWARE** – Software obtained through public sources with normally limited features, periodic visual reminders to purchase, or a time limit cutoff to prevent use without purchase.

**VIRUS** - A self replicating computer program capable of attaching itself covertly to files. Can also be an executable program designed to perform actions not authorized by the system's user, i.e. making the system mail the virus to the first 50 people in the user's address book.

**WORLD WIDE WEB** - A portion of the Internet that transmits information in the form of text, graphics, sound and video.

**WORM** - A computer program designed to covertly destroy or manipulate data, but cannot attach itself to other programs. A worm still replicates itself to other computers and uses memory, but will always arrive in the same program.

### **III. ADMINISTRATIVE GUIDELINES**

- A. These policies apply to all members of the Pine Bluff Police Department utilizing Department computer equipment or Department computer systems. Use of these systems implies that members agree to comply with all applicable policies, guidelines and laws regarding their use.
- B. A Systems Administrator will be assigned the responsibility for all computer security, access and the operation of computer systems utilized by the Pine Bluff Police Department. Each employee will use a unique password and system login as designated by the Systems Administrator. [CALEA 82.1.9]

- C. The Systems Administrator shall be the only Department employee authorized to issue user login and passwords and shall determine, based upon the user's duties, the level of access to computer systems. [CALEA 82.1.6]
- D. The Systems Administrator shall be responsible for backing up computer systems daily. Other backup routines may be performed as needed. Backup tapes will be stored in a secure area maintained by Systems Administrator. [CALEA 82.1.8]
- E. Only the Information Technology Section personnel, or their designee, will install hardware/software on Department computers.
- F. The Administrative Services Division is responsible for granting and monitoring access to Department computer systems by issuing each Department member a "computer account." A member is prohibited to use any "computer account" which is assigned to another person, without permission from a supervisor.
  - 1. Example: Someone not authorized to use the internet uses another employee's computer system that is authorized. An authorized breach of the Department's computer system security is considered a Cardinal Offense.
    - a. If without the authorized user's knowledge, the unauthorized user may be subject to disciplinary action as determined by the Chief of Police or their designee.
    - b. If with the authorized user's knowledge, both employees' can be liable for disciplinary action as determined by the Chief of Police or their designee.
- G. Members are responsible for their own network account, **regardless of who actually uses it**; therefore, they are responsible for logging off the network upon completion of their computer activity.
- H. As stated above, members must have and use their own login and passwords to access the network. Login and passwords should be a combination of letters, numbers, or symbols, and should not be obvious, such as a serial number or a birthday. Disclosure of login and passwords, access codes, or other authentication devices to other members must be kept to an absolute minimum and done only when approved by a supervisor. This is one aid in preventing a security breach.
- I. Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. The **ability** to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy the file.
- J. Users may not use the Department computer systems to invade the privacy of other department members by unnecessarily reviewing their files and e-mail.

- K. Members will not use the Department computer system to harass, make defamatory remarks towards others, or perform illegal or malicious acts.
- L. Members will not interfere with or disrupt any Department computer system, Internet user, program, or equipment. Disruptions include but are not limited to propagation of computer worms, viruses, or other debilitating programs, and using the Department computer system to make unauthorized entry to any other machine accessible via the computer system or Internet.
- M. Viruses can cause substantial damage to the Department computer systems. Each user is responsible for taking reasonable precautions to avoid introducing viruses to Department computer systems.
  - 1 Files obtained from any source outside the Department, including computers or floppy disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by vendors, may contain dangerous computer viruses.
  - 2 Users should never use disks from non-department sources or download Internet files or accept e-mail attachments from unknown sources without first scanning the material with Department installed virus software. If a user suspects that a virus has been introduced into the Department network, he/she should notify their supervisor and Information Technology Section or the Department's System Administrator immediately.
- N. Members, who become aware of any computer system security breach, whether internal or external, will **immediately** notify their supervisor and the Administrative Services Division. Software/hardware manipulations will be reported to the Information Technology Section for training, procurement and managerial decisions.
- O. Any member observing someone using the Department computer system inappropriately will notify his/her commander/supervisor. The commander/supervisor receiving such information will review it and take appropriate action.
- P. Data saved on a networked computer is automatically backed-up (copied) on the server; however, members are responsible for making back-up copies to another source such as the hard drive and/or a floppy disk. Members saving data on a non-networked computer are responsible for making back-up copies to a floppy disk.
- Q. Commanders and supervisors will ensure that all personnel with personal computer access, who are assigned to their elements, are knowledgeable of the guidelines and procedures addressed in this policy.
- R. Those employees who have State and National computer system security shall access those files and records in accordance with specific training provided for the use of the State and National computer systems.

- S. Information retrieved from State and National computer files and the National Law Enforcement Telecommunications Network (N.L.E.T.S.) is intended for official police use only and the dissemination of this information to non-criminal justice individuals is strictly prohibited and could subject the offender to criminal and civil penalties [§ 12-12-212]. [CALEA 82.1.1d]
- T. Each employee who has State and National computer access must attend a re-training session every two years to maintain security authorization. Failure to attend a bi-annual training session will result in access to these files being temporarily suspended and the employee being required to attend the basic Terminal Operator course to obtain certification.
- U. Any employee who disseminates Criminal History information from any State or National computer system must log that dissemination into a Criminal History log which shall be maintained within areas where State and National Criminal History information may be gained. [CALEA 82.1.9]
- V. Dissemination of Criminal History information as described above must be to Criminal Justice officials, outside the PBDP organization, authorized to receive Criminal History information. [CALEA 82.1.9]
- W. The Criminal Justice official receiving the information must be identified by Organization, name employee number or social security number, address and phone number along with the date and time the information was disseminated. [CALEA 82.1.9]
- X. Completed Criminal History log sheets shall be maintained in the Criminal History logbook until such time as designated members of the Management Research Unit collect them. **Criminal History logs must be available for inspection during normal business hours.**

#### IV. PROCEDURES

This directive has been arranged in annexes to address the various areas of concern which are pertinent to the security, privacy, and integrity of the Department's computer systems.

- 1 Annex A Personal Computers
- 2 Annex B Electronic Mail (E-Mail) Communications
- 3 Annex C Internet Usage
- 4 ANNEX D Mobile Data Computers and Mobile Data Terminals

**DISTRIBUTION:**

Law Enforcement Personnel  
Civilian Personnel

**ANNEX A**

**PERSONAL COMPUTERS**

**I. INTRODUCTION**

The security of the Department's computer system is of paramount importance in maintaining an efficient and well-guarded database for referencing computerized information. Users will strictly adhere to the following guidelines on the usage of personal computers and associated software to ensure compliance with federal copyright laws and protection against computer viruses.

**II. POLICY**

- A.** The use of software/hardware on Department personal computers will be limited to lawful and productive endeavors.
1. The unauthorized copying of personal computer software is prohibited.
  2. The Information Technology Section or their designee will evaluate all requested hardware/software changes, and if compatible, will be responsible for installation.
  3. To ensure proper software/hardware licensing and compatibility requirements, **only** members of the Information Technology Section their designee, or authorized network administrators will install hardware/software on **any** Department computer.
  4. When required for legal compliance, all software installed on Department computers will be registered or licensed with the software manufacturer. Copies of the registration and/or license agreement will be forwarded and maintained in the Information Technology Section
  5. Shareware software will not be utilized on Department computers for a time period in excess of that allowed by the manufacturer for trial purposes, unless it has been purchased and properly registered. All shareware software must be reviewed by the Information Technology Section prior to being installed on any Department computer.
  6. Freeware software will only be installed on Department computers when it has been ascertained that such software is usable by government organizations free of charge. All freeware software must be reviewed by the Information Technology Section prior to being installed on any Department computer.

- B. Department computer equipment, peripherals, and components will be utilized for Department business only.
- C. Only Information Technology Section personnel, or an approved designee, will move, install or disassemble Department computer equipment.
- D. The Information Technology Section will install antiviral software on all Department computers.
  - 1. Members should be aware of the potential for viruses when using floppy disks in different computers. The computer or disk may become contaminated with a virus simply by inserting the floppy disk and opening a file.
  - 2. Members should regularly scan their computers and floppy disks for viruses and report any viruses that the computer is not able to repair itself to the Information Technology Section during regular business hours.
- E. Members with proper authorization may utilize privately owned personal computer equipment for Department business.
  - 1. Privately owned computers will not be connected to the Department network.
  - 2. Members will be responsible for and adhere to Department computer policies when utilizing privately owned computers.
  - 3. Personal hardware components, such as printers, external modems, external drives, etc., **will not** be connected to Department equipment.
  - 4. Technical support on privately owned computers for **Department business** will be considered on a case by case basis.

**ELECTRONIC MAIL (E-Mail) COMMUNICATIONS**

**I. PURPOSE**

To establish procedures for the creation, dissemination, and storage of all Intranet and Internet electronic mail messages and to set guidelines for their content.

**II. ADMINISTRATIVE GUIDELINES**

- A.** Use of the e-mail system by any member implies both understanding and compliance with this directive. Members using the e-mail system will do so in an appropriate and professional manner. Any member observing someone using the e-mail system inappropriately, or who receives unusual or inappropriate material, will notify his/her commander/supervisor. The commander/supervisor receiving such information will review it and take appropriate action.
- B.** All messages generated on or handled by the Department e-mail system, including back-up copies, are considered property of the Department, not the member.

**III. PROCEDURE**

- A.** The Department e-mail system generally should be used for official use only. Incidental personal use is permissible as long as it does not interfere with productivity or preempt official use.
- B.** Every Department member is encouraged to use the e-mail system when appropriate. Appropriate uses include, but are not limited to:
  - 1.** Routine messages, announcements, notices, or other information that previously would have been disseminated via memorandum through the chain of command or by inter-department mail.
  - 2.** Any message currently being sent via facsimile, by voice over the telephone, or over a paging system.
  - 3.** Drafts of reports, projects, or proposals.
  - 4.** Certain non-confidential Department documents such as Job Vacancies, Department Memorandums, Bureau Memorandums, or Special Orders.



- C. Unless approved by the Chief of Police or designee, the e-mail system **will not** be used for:
1. Disseminating confidential materials or Department sensitive information, official documents that must be retained in their physical form, or documents that require a physical signature to certify receipt.
  2. Charitable endeavors.
  3. Private business activities.
  4. Inappropriate entertainment purposes.
- D. Members will not use obscene, racist, or sexist language in e-mail and will not transmit threatening or harassing materials (i.e., jokes, photographs, or programs forwarded as attachments), nor engage in any form of sexual harassment.
- E. Every member using the e-mail system should check their e-mail box on a regular basis to ensure timely dissemination of information.
- F. Every member using the e-mail system will be able to store a limited number of e-mail messages within the system. If storage space becomes limited, a member will be required to remove all messages which are not required to be saved.

G. **SECURITY/PRIVACY**

1. E-mail messages sent or received by Department employees are **not** private and the Department reserves the right to monitor all email messages without notification to the member; however, it is not the Department's intent to monitor all e-mail messages. It is a violation of this policy for any user, including the system administrator or any supervisor, to access the e-mail system or message merely to satisfy curiosity about the affairs of others.
2. E-mail messages created in the course of public business are, for the most part, a public record. Those messages are subject to inspection by the news media and other members of the public, unless the sender has marked them confidential. **Every e-mail message should be both professional and courteous.**

**INTERNET USAGE****I. PURPOSE**

To establish procedures for ensuring the appropriate protection of Department information and equipment by Internet connections.

**II. ADMINISTRATIVE GUIDELINES**

Use of Internet by any member implies both understanding and compliance with this procedural instruction. Internet access is only authorized for official Department business and users are expected to know the tools, rules, and etiquette of the Internet. Any member observing inappropriate use of the Internet will notify his/her supervisor/commander. The supervisor/commander receiving such information will review it and take appropriate action.

**III. PROCEDURE**

- A.** Employees must use the Internet in accordance with all applicable laws and regulations. This includes compliance with copyright and license laws governing programs, as well as data and written materials accessed, obtained or provided to others via the Internet.
- B.** Members will not download software from the Internet without prior approval from PC Support. **Note:** To prevent inadvertent downloading, Internet users should be wary of pop up menus or advertisements that suggest doing so.
- C.** All software that is approved to be downloaded from non-Department sources via the Internet will be screened with virus detection software prior to being opened or run. Whenever the provider of the software is unknown or not trusted, it should be tested on a stand-alone non-production machine and not one that is connected to the network.
- D.** Members will not place Department material (internal memos, etc.) onto the Internet without prior approval of the Chief of Police or his designee.
- E.** Prohibited uses of the Internet include but are not limited to the following:
  - 1.** Using Internet connections for private gain or profit, or to solicit for political, religious, or other non-business purposes.
  - 2.** Violating the privacy of others. Members must be sensitive to the fact that Internet news group postings, some e-mail messages, web sites, and various other communications on the Internet are public information.

3. Using obscene, offensive, racial, sexual or hate language or images; engaging in ridicule; transmitting threatening, racial, sexual, obscene or harassing materials; engaging in any form of sexual harassment.
4. Interfering with or disrupting any Department network, Internet user, program, or equipment. Disruptions include but are not limited to propagation of computer worms, viruses, or other debilitating programs, and using the Department network to make unauthorized entry to any other machine accessible via the network or Internet. Deliberate attempts to degrade or disrupt system performance may be considered criminal activity with possible prosecution under applicable state and federal laws.
5. Deliberately accessing pornographic or Internet gambling web sites.  
**Exception:** This does not apply to investigative units during the course of approved criminal or Departmental investigations.

**F. SECURITY/PRIVACY:**

The use of the Internet is **not** a private matter and the Department reserves the right to monitor all uses without notification to the member; periodic audits will be conducted by the Administrative Services Division.

**MOBILE DATA COMPUTERS AND MOBILE DATA TERMINALS**

**I. INTRODUCTION**

The security of the Department's computer system is of paramount importance in maintaining an efficient and well-guarded database for referencing computerized information. Users will strictly adhere to the following guidelines on the usage of Mobile Data Computers and PC compatible Mobile Data Terminals, regardless of type, make, or manufacturer and associated software to ensure compliance with federal copyright laws and protection against computer viruses.

**II. POLICY**

- A.** Mobile Data Computers and PC compatible Mobile Data Terminals, regardless of type, make, or manufacturer, have been installed in police vehicles to assist officers in the execution of efficient police functions and to reduce the amount of radio traffic necessary to conduct police operations.
- B.** Officers have been trained in the use and care of both the M.D.C. and M.D.T. and are expected to use this equipment in accordance with instructions provided. M.D.C.s and M.D.T.s were designed and have been programmed to provide information from State and National computer files on persons, vehicles and other property. [CALEA 81.2.9]
- C.** Officers shall use the M.D.C./M.D.T. to check information on persons, vehicles, and other property and shall not request these types of transactions be conducted by Central Communications. The only exceptions to this Order will be when an officer needs a printout of the information for inclusion with other reports or does not have an M.D.C./M.D.T. or the M.D.C./M.D.T. is not functioning properly.
- D.** If the unit is not functioning properly, officers are expected to request repairs as soon as possible during the normal working hours of the Office of Management Support or the next business day the Office of Management Support is open.
- E.** M.D.C./M.D.T.s have also been programmed to allow for communication of official police business between police vehicles and between field units and Central Communications. No vulgar, obscene, or derogatory messages, racially and/or sexually derogatory remarks shall be transmitted via the M.D.C./M.D.T., nor shall any private, non-police business conversations be conducted between units through the M.D.C./M.D.T. All transmissions are logged into the mainframe system and a copy of each day's transactions are maintained for future reference and to provide education and training as deemed necessary.

- F. Officers shall log on with their designated log on name and User-ID. Officers shall not use another officer's log on name and User-ID. At the end of shift, officers shall log off the M.D.C./M.D.T. system.
- G. Mobile Data Computer and Mobile Data Terminal transmission log review [CALEA 41.3.7]
- H. Transmissions from each Mobile Data Computer and/or Mobile Data Terminal are electronically logged into a file accessed by Management Research personnel. A copy of each day's activity is retrieved by Management Research personnel and stored on an electronic media.
- I. Each Division Commander where Mobile Data Computers and/or Mobile Data Terminals are deployed shall review, on a monthly basis, the transmission logs for security violations, transmissions which violate the procedures enumerated in this General Order and for the need for disciplinary action or further training on the use of the device.
- J. Prohibited uses of the Internet include but are not limited to the following:
  - 1. Using Internet connections for private gain or profit, or to solicit for political, religious, or other non-business purposes.
  - 2. Violating the privacy of others. Members must be sensitive to the fact that Internet news group postings, some e-mail messages, web sites, and various other communications on the Internet are public information.
  - 3. Using obscene, offensive, racial, sexual or hate language or images; engaging in ridicule; transmitting threatening, racial, sexual, obscene or harassing materials; engaging in any form of sexual harassment.
  - 4. Interfering with or disrupting any Department network, Internet user, program, or equipment. Disruptions include but are not limited to propagation of computer worms, viruses, or other debilitating programs, and using the Department network to make unauthorized entry to any other machine accessible via the network or Internet. Deliberate attempts to degrade or disrupt system performance may be considered criminal activity with possible prosecution under applicable state and federal laws.
  - 5. Deliberately accessing pornographic or Internet gambling web sites.  
**Exception:** This does not apply to investigative units during the course of approved criminal or Departmental investigations.

**G. SECURITY/PRIVACY:**

The use of the Internet is **not** a private matter and the Department reserves the right to monitor all uses without notification to the member; periodic audits will be conducted by the Administrative Services Division and/or the Office of Professional Standards.