

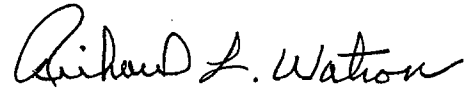
FAYETTEVILLE POLICE DEPARTMENT  
FAYETTEVILLE, ARKANSAS 72702

**GENERAL ORDER # 09**

**SUBJECT:** Computer Information Security

**CROSS-REFERENCE:**

**DATE APPROVED BY COP:** October 5, 1999

  
Chief Richard L. WATSON

**PURPOSE:** All police computer systems, (including but not limited to the IBM mainframe, Computer Aided Dispatch system, Mobile Computer Terminals, Personal Computers, Department LAN system, Laptops, ACIC terminals and access to the City Pass-through), hardware and software, are for the official use of Police Department employees only and are intended to improve the efficiency and quality of departmental operations.

**ORDER:** Operation of the above systems must be in accordance with established security measures as outlined below and shall be limited by security access as determined by the employees Division Supervisor. Records and information maintained by the Fayetteville Police Department are for the exclusive use of departmental employees only and shall only be disseminated to persons affiliated with a bona fide law enforcement agency or as directed by Police Department Administration.

**PROCEDURES:**

**A. Security for Computer System**

1. Each employee shall log onto the IBM mainframe system and those authorized to access the Computer Aided Dispatch System with their own unique User-ID number and password shall access only those files and records as specified by their security level and job description. When not in use, the system should be logged off to prevent unauthorized use.
  - a. No employee shall attempt to modify any record or file which would be illegal or which tends to impair the operation of this department in its administration of justice. No employee shall attempt to delete any file or record contained in the IBM mainframe system or the Computer Aided

Dispatch system unless authorized to do so. Attempts to modify or delete any file or record, which tends to impair the operation of this department, may result in disciplinary action being initiated against the offender.

- b. All entries, inquiries, modifications and attempted deletions are recorded in electronic history logs, which are maintained and reviewed by the Systems Analyst.
- c. Use of Data Utility Tools on the IBM mainframe are strictly forbidden without prior approval from the Information Systems Coordinator. In cases where approval is given for the use of these tools, both electronic and paper logs will be generated and maintained by the Systems Analyst.
- d. No employee shall use another employee's User-ID and password nor shall any employee attempt to secure the User-ID and password of another employee. All department employees issued passwords are directed to keep their passwords secret from other persons.
- e. 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 State and National computer systems.
  - 1. Information retrieved from State and National computer files 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 penalties.
  - 2. 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 the employee being required to attend the basic course to obtain re-certification.
- f. All requests for new IBM programs or applications or the modification of current programs, applications or advanced information searches, shall be forwarded through the employee's chain of

command to the Systems Analyst.

- g. All requests for assistance, equipment repair, investigations of file activity or mistakes on the part of any employee or specific user information shall be routed through the Systems Analyst.
  - h. Any supervisor who needs additional training for their employees or any employee who desires additional training on the IBM mainframe system, Computer Aided Dispatch System, Mobile Computers, or Windows 95 products, should contact the Systems Analyst to schedule the requested training.
1. Certain personnel will be given Internet access. The Internet will be accessed on department computers for bonafide work purposes only. The access of Chat Rooms or Pornographic material (except for official police department business) is expressly prohibited.

**B. Mobile Computer Terminals (MCT)**

- 1. Rocky II and Panasonic Laptop Personal Computers 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.
- 2. Officers have been trained in the use and care of the MCT and are expected to use this equipment in accordance with instruction provided. MCT's have been programmed to provide basic information from the IBM mainframe and aid in the collection of reports in the field.
  - a. Officers should use the MCT to check information on persons, vehicles and other property and refrain from requesting these types of transactions from Dispatch.
  - b. The only exceptions to this Order will be when an officer needs a printout of the information for inclusion with other reports, does not have access to an MCT, the MCT is not functioning, the mobile interface is down or when officer safety would be compromised.
  - c. If the unit is not functioning properly, officers are expected to request repairs through their normal chain of command.

- d. If the mobile system interface is not working, officers are expected to notify the Information Systems Coordinator or Dispatch.
3. MCT's have also been programmed to allow for communication of official police business between police vehicles and between field units and Dispatch.
    - a. No vulgar, obscene, or derogatory messages, racially and/or sexually derogatory remarks shall be transmitted via the MCT, nor shall any private, non police business conversations be conducted between units through the MCT.
    - b. All transmissions are logged into the Message Switch System (RS6000) and transactions are maintained for future reference and to provide education and training as deemed necessary.
    - c. Officers are discouraged from conducting transmissions on the MCT while driving. This does not pertain to two person units with the passenger entering the transactions.
  4. Officers shall log on with their designated User-ID and password. Officers shall not use another officer's User-ID and password. At the end of each shift, officers shall log off the MCT.

**C. Departmental Personal Computers and Laptops**

1. The use of all departmental personal computers and laptops shall be for official Fayetteville Police Department business.
2. Employees shall ensure all computer equipment is kept clean and shall request necessary repairs or replacement through their chain of command.
3. Many departmental personal computers and laptops have been designated to be used by specific individuals. The unauthorized use of departmental personal computers or laptops, the unauthorized deletion of files or applications, or installation of new software into a designated personal computer or laptop is not permitted without proper authorization.
4. No personal software should be brought into the Department from other sources and should not be

loaded onto any of the department's personal computers or laptops.

5. No diskettes are to be brought in from other departments or home without being properly scanned by our Systems Analyst for viruses.
6. All departmental personal computers and laptops are subject to be inventoried by authorized employees and all programs on any departmental personal computer or laptop must be authorized and have appropriate documentation to verify authenticity.
7. The addition or modification of programs or hardware on any departmental personal computer or laptop must be coordinated through the Systems Analyst.