SUPPORT SERVICES

COMPUTER SYSTEMS

Purpose: The purpose of this directive is to regulate the use of computer equipment by agency members and set forth procedures for maintaining physical security and data integrity for the equipment.

Policy Statement: The North Little Rock Police Department utilizes computer equipment to aid in accomplishing its primary mission of preventing crimes and apprehending criminals. Access control and system backup are critical to maintaining the integrity of the computer system and will be administered and maintained by the Professional Development Division's Information Technology Unit.

Summary of Changes: New format.

1 Procedure:

1.1 Computers and related equipment owned or operated by or for the North Little Rock Police Department will be used for official Department business only.

1.1.1 Members may make off-duty personal use of Department computers for professional and career development purposes with prior notice given to the appropriate supervisor.

1.2 Members must use their assigned password to log onto the system. Members should not reveal their password to any other member or leave it in written form accessible to other persons.

1.2.1 Members are responsible for all transactions made in the system under their user ID and password.

1.3 Members should log off the system or secure their computers while unattended.

1.4 Members will receive the training, as needed, to operate assigned computers and the requisite programs required to perform their job functions.

1.5 All software used in Department computers will be installed and used in accordance with the software license agreement. Only Department owned or approved software may be installed in Department computers. [CALEA 11.4.4]

1.5.1 Game software will not be installed in Department owned computers.

1.6 Only members assigned to the Department's Information Technology (IT) Unit, or persons authorized by the IT Unit, will be authorized to install software in any computer connected to the Department's network.

1.6.1 Members will contact the IT Unit for authorization to install personally owned software in a Department computer.

1.7 The IT Unit will be responsible for periodically checking all Department computers for compliance with software license requirements. Any unapproved software or software found installed in violation of software license agreements will be properly licensed or removed from the computer.

2 Restrictions

2.1 The use of Department owned computer equipment is solely for purposes authorized by the Department. Unauthorized use is a violation of these policies and procedures, and violators will be subject to disciplinary action.

2.2 Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

2.3 Software and databases used in the Department's data processing are property of the City of North Little Rock and will not be loaned, traded, sold, given away, or otherwise divulged without permission from the Chief of Police or his designee.

2.4 Only software that has been approved by the Department in accordance with operational needs is allowed on the Department's data processing systems. Any unauthorized software, such as games and other personal amusement software, will be deleted.

2.5 Members will not intentionally remove any network wiring without authorization from the IT Unit.

2.6 Computer equipment connected to the Department network will not be disconnected or moved without authorization from the IT Unit.

3 Security

3.1 The Department's data processing equipment will be located in a secure location with controlled access by authorized members only.

3.1.1 The IT Unit will maintain an inventory of the data systems hardware and software and check it on an annual basis.

3.2 The Department provides various layers of technical protection to safeguard data and software, including programs that allow IT personnel to monitor uses of the Department's data processing systems to provide an acceptable degree of security to accomplish the following:

3.2.1 Detect illegal penetration and prevent unauthorized access to the data processing systems;

3.2.2 Prevent unauthorized access to stored data;

3.2.3 Determine unauthorized use of internet and intranet network capabilities of the data processing systems.

3.3 Duplication and off-site storage of critical Department data will be conducted by the IT Unit.

3.3.1 Members are encouraged to back up their own data to protect against data loss in the event of power outages or system failures.

_____

Mike Davis
Chief of Police