NORTH MIAMI POLICE DEPARTMENT

STANDARD OPERATING PROCEDURES

COMPUTER SYSTEMS 100.06

EFFECTIVE DATE: 07-08-22

APPROVED: _____
Chief of Police

SUPERSEDES: 02-07-20

CFA: 26.04, 32.01

CONTENTS:

I. PURPOSE

To ensure the efficient and effective use of Department-issued computer hardware and software in accordance with Federal, State, and local legal guidelines.

II. POLICY

All Department personnel assigned and/or given access to any Agency computer hardware and software must also abide by the City of North Miami's Administrative Regulation 1-75, to include its directives on security, emails, Internet and laptop use.

III. SCOPE

This policy applies to all members of the Department, to include School Safety Officers (SSO), detached task force members, and any member utilizing Agency computer hardware and software equipment outside of the Agency for law enforcement activities.

IV. GENERAL RESPONSIBILITIES

A. The desktop and mobile laptop computers, all attached equipment, computer software and data files are the property of the City of North Miami.

B. Passwords assigned to or used by employees do not create an expectation of privacy for the employee, but are used solely to prevent access by unauthorized persons; therefore, employees shall have no expectation of privacy when using Department authorized or provided communications through its computer systems.

C. Responsibilities:

1. Administrative Section: The Administrative Section Major, or designee, shall be responsible for the overall implementation, control, and maintenance of the Department's computer system, both desktop and laptop.

2. Supervisors: Supervisors shall ensure that their respective personnel are properly trained in the use of the mobile laptop computers. They shall ensure that the computers are properly cared for, secured, and used in a manner that is consistent with Departmental policy. The City of North Miami Information Technology (I.T.) staff will conduct quarterly inspections of the mobile laptop computers assigned to their personnel to ensure that they are being maintained properly. Damage and/or deficiencies will be documented by memorandum to the Administrative Section Major via the chain-of-command.

3. The I.T. Department will assign a Network Specialist (or other qualified personnel) to provide system administration and daily problem resolution. The Network Specialist shall report to the Administrative Section Major or designee.

4. Members assigned a mobile laptop and/or desktop computer, including any related accessories, whether on a permanent or temporary basis, shall be solely responsible for the care and safeguarding of said items.

5. Repairs and/or other issues with City-owned computers and software will be addressed as follows:

a. Using the City's Intranet (Internet Explorer), go to the I.T.

Department and create a New Ticket. The repair or problem with the computer will be recorded and the I.T. Department will route the ticket to the Police Department's Network Specialist for repair.

V. AUTHORIZED USE

Department computer hardware, software, and related accessories, will be authorized for use as follows: **CFA 32.01E**

A. Report Writing: The primary use of the mobile laptop computers is intended for the writing and transmission of completed police reports. All initial and supplemental reports will be written on the computers as opposed to handwritten, unless precluded by circumstances, and only when authorized by a supervisor. Reports will be generated in accordance with established criteria.

B. Criminal Information Systems: The mobile laptop computers interface with the Florida Criminal Information Center (FCIC) and the National Criminal Information Center (NCIC). Departmental members will be aware that Florida State Statutes, as well as the Florida Department of Law Enforcement (FDLE) regulate access to FCIC/NCIC. Use of information in the system is strictly limited to law enforcement purposes and may not be disseminated to any person for any other purposes. Use of the FCIC/NCIC network is restricted to personnel who have received FCIC/NCIC training and hold an active certificate.

1. Members having access to and use of personal identification information will follow all pertinent legal guidelines as instructed during training pursuant to FSS 817.568, which addresses the criminal use of personal identification information. **CFA 32.01F**

C. Unit-to-Unit Communications (Electronic Messaging): The mobile laptop computers have the capability to communicate car-to-car and car-to-station. All communications via the mobile laptop computers are logged in the mobile network server for routine storage. These records are subject to disclosure under Public Record laws and members should restrict all such communications to official business. The use of language or images that could be considered lewd or offensive are strictly prohibited.

D. Email Use: Department members will abide by the City's Administrative Regulation 1-75, to include the user E-mail responsibilities (Section VII, D) noting that users assigned an E-mail address shall check their E-mail

at a minimum once each working day. **CFA 32.01A**

E. Other Uses: There may be circumstances when Department members will need computer software applications to facilitate their assigned duties. The loading of all computer software must be approved in writing by the Administrative Section Major, or designee. All software must be fully licensed for use and free from viruses or malware. **CFA 32.01C**

1. The Department will not be responsible for the loss of a member's personal information files or programs from mobile laptop computers whether intentionally deleted by the Department or I.T. personnel, or through the failure of hardware, software, or electrical components.

2. Nothing, other than work-related software, may be loaded on Department computers. **CFA 32.01C**

3. Department personnel shall not modify, add or delete any settings, components or files on the laptop computers, unless authorized to do so by the Network Specialist, Administrative Section Major, or designee. Personnel are specifically prohibited from altering or modifying the system files and settings. Personnel shall not allow any other person to modify, add or delete any settings, components or files, other than when authorized as above.
CFA 32.01C-E

4. Department computers will be subject to inspection by I.T. staff to ensure proper use and maintenance. Department-related files will not be hidden or password protected. Personal files will be inspected in accordance with Section XI of this policy.

5. Access and Use Restrictions: **CFA 32.01D**

a. Use of Department-owned computers and software is restricted to Department members and authorized members of the I.T. Department.

b. The use of Department mobile laptop computers is restricted to on-duty personnel, or personnel working authorized Off-Duty police work, and can only be used for work-related activities.

c. Information obtained through Department-accessed programs is for criminal justice purposes only. Under no circumstances will the following databases be accessed for personal use:

1). FCIC/NCIC

2). County Local Computer
3). NMPD Records Management System
4). D.A.V.I.D. (Driver and Vehicle Information Databases)
5). E.L.V.I.S. (Electronic License and Vehicle Information System)
6). Dataworks

VI. DATA SECURITY

The following safeguards will be followed to protect all Departmental electronic information against unauthorized attempts to access, alter, remove, disclose or destroy stored information: **CFA 26.04A**

A. Members will not access files on laptops not assigned to them, unless specifically authorized by the person to whom the laptop is assigned. Any damage to the computer or problems with the programs shall be reported immediately to their supervisor or shift commander. **CFA 32.01D**

B. All transactions through the mobile data system are stored electronically and are retrievable from the mobile data system server by authorized personnel only.

C. Information transmitted through the mobile data system should be considered as CONFIDENTIAL. However, this information may be utilized in court, for administrative functions, or may be released pursuant to public records requests and court orders. Any requests for access to this information shall be directed to the Administrative Section Major, or designee.

D. Department employees shall secure their vehicles to preclude the theft of, unauthorized use, or tampering with their mobile laptop computers. Employees shall "logoff" from all applications at the end of each shift or whenever the vehicle will be left unattended.

E. Laptop computers are accessed solely through a dual authentication process, using a secure password and, if applicable, fingerprint of the member assigned to the laptop. Members will not disclose confidential passwords to anyone unless authorized to do so by supervisory personnel, or the I.T. Network Specialist. **CFA 32.01D**

F. Laptop computer wireless communication devices shall not be used to access the Internet, or any other on-line service, unless for work-related activities. **CFA 32.01B**

G. The Network Specialist will be notified as soon as possible when an employee separates from service, and he or she will deactivate all electronic access to the City's computer systems within two (2) business days. **CFA 26.04C, 32.01D, E**

VII. RULES OF CONDUCT

A. Agency desktop and mobile laptop computer hardware and software systems shall be used for work-related purposes only.

B. Department computers and software shall not be used to commit any act that may discredit or negatively impact the reputation of the Department.

C. Messages shall be limited to official business and shall not contain profanity, text or images of a sexually explicit nature, or in any way constitute degrading or insulting personal remarks or innuendoes towards any Department member, or other persons.

D. Anyone member who violates these Rules of Conduct may be denied access to the mobile data system and be subject to disciplinary action.

VIII. SAFETY ISSUES

A. The voice dispatch procedures are the primary means of assigning calls, officers advising their status, and any other communications relative to calls for service. The laptop computer network shall not be used as the primary means of dispatch/communication, unless due to a failure of the radio system and only with authorization from a supervisor.

B. All information pertaining to officer safety shall be voice broadcast unless doing so would jeopardize officer safety.

C. Drivers of vehicles utilizing laptop computers should not use the laptop computer while the vehicle is in motion.

D. Officer-initiated activities that involve the investigation of suspicious activities, or any potential officer safety concerns, must be reported to the dispatcher.

IX. DISTRIBUTION AND ASSIGNEMENT OF MOBILE LAPTOP COMPUTERS

A. Permanently Assigned Units: Individual members will be assigned a

mobile laptop computer for their use. Officers assigned to the Uniform Patrol Section will be given priority in the assignment of the mobile laptop computers. The Administrative Section Major, or I.T. staff, will assign the computers and maintain a description and serial number of the unit. Upon reassignment to a different unit or section, or upon separation from the North Miami Police Department, all members will return his/her computer to the Administrative Section Major or designee.

B. Spare Units: Whenever possible, the Department will maintain spare mobile laptop computers for temporary assignment to members. The following guidelines will pertain to the assignment of those computers:

1. Spare computers will be assigned by the I.T. Network Specialist who will be responsible for documenting the name of the individual to whom it is being assigned and the date and time assigned.

2. The I.T. Network Specialist shall ensure that returned laptop computers are functional and any damage to the unit(s) is fully documented. Previously undocumented damage will be reported immediately in writing to the Administrative Section Major along with an explanation as to how the damage occurred.

X. REPAIR AND MAINTENANCE OF MOBILE LAPTOP COMPUTERS

A. Fresh damage to a mobile laptop computer must be reported to the member's immediate supervisor prior to the end of the shift the member is working. If the unit is not operable, the member must immediately notify his/her supervisor and turn the unit in for repair/replacement. The supervisor will forward a written report to the Administrative Section Major documenting the damage and the circumstances under which it occurred.

B. Malfunctioning units will be turned in to the Police Department's I.T. Specialist. If the network specialist is unavailable, the damaged unit(s) will be locked in a property locker.

XI. INSPECTIONS

A. Mobile laptop computers, hardware, software, and data files relating to official Departmental operations shall be subject to routine periodic inspection by supervisory personnel. Inspection of members' personal files shall be conducted only upon the direction of the Chief of Police, or his/her designee.

B. Employees who are found to have operated any computer hardware or software in violation of this policy may be subject to disciplinary action.

XII. FILE MAINTENANCE

A. The City of North Miami I.T. Department will ensure computer files are maintained, secured and backed-up on a nightly basis, and will be retained in accordance with Public Record Laws. **CFA 26.04B**

B. Requests to restore backed-up documents will be directed to the City's I.T. Department.