MOBILE DATA ACCESS

1. PURPOSE: The purpose of this Written Directive is to establish procedures to be followed when using departmental issued mobile data access equipment.

2. SCOPE: This written directive is applicable to all personnel.

3. RESPONSIBILITIES: All employees will comply with this written directive.

4. DEFINITIONS

   A. MOBILE DATA ACCESS EQUIPMENT - The tablet/laptop computers issued by the Department and used by personnel in field operations. This includes all accessories which enable the computer to be functional (e.g., computer, mounts, radios, antennas, and related cabling).

   B. AUTOMATIC VEHICLE LOCATION (AVL) – Automatic vehicle location equipment that uses cell tower signals to pinpoint the location of a vehicle, and relays that information to the Department's computer dispatching system.

5. PROCEDURES: Department personnel will use their issued tablet/laptop each time they drive a vehicle that is equipped with a tablet/laptop mount. This can be either their assigned vehicle or a spare vehicle that is similarly equipped.

   A. USE OF TABLET/LAPTOP REQUIRED: Employees shall dock and log on to their assigned tablet/laptop computer each time that they operate their assigned vehicle and/or a similarly equipped spare vehicle. This will include regular duty, extra duty, court appearances, and vehicle maintenance.

   B. DURATION: Officers will ensure that they are properly logged on to the computer, and the Mobile for Public Safety (MPS) program is running prior to driving the assigned vehicle. They will remain logged on to the computer until they finish their assigned duty and are at their residence or the precinct where they park their vehicle when not on duty. (If technical problems occur that make it impossible to comply with this section, a supervisor will be immediately notified, and corrective action will be taken to repair the equipment as soon as possible).

   C. LOGGING ON TO MPS: Officers will log on and remain logged on to the MPS program when going in service for regular duty, extra duty, court appearances, and vehicle maintenance.

      NOTE: When two officers ride together (e.g., dual, FTO program, etc.), the officers shall ensure both of their employee numbers are logged into the MPS program.

   D. STATUS MARKERS: After logging on to the MPS program, Officers will ensure that the

MPS program is displaying green status marker for the connection to the 911 center. This status marker is displayed on the bottom right of the screen, next to the "GPS" indicator. Officers will ensure the GPS indicator is lit up in white meaning it has a connection to the AVL.

E. MALFUNCTIONS: If any of the markers do not show the correct status, a supervisor will be notified, and appropriate action will be taken to ensure that all of the installed equipment is functioning properly. If the AVL status is not lit up in white, dispatch will be notified via the police radio system. If the supervisor cannot remedy the situation, the assigned officer will have the vehicle and tablet/laptop checked by the appropriate service personnel as soon as is possible.

F. DISPATCH REQUIREMENTS: If a dispatcher becomes aware that an officer's AVL is not functioning properly, the dispatcher will immediately notify the officer's supervisor. The supervisor will then take the appropriate action to have the situation remedied.

G. DISABLING AVL: At no time will an officer turn off, disable, tamper with, or in any way attempt to interfere with the proper operation of the AVL system.

H. MESSAGING CAPABILITIES: Electronic messages are not private or confidential. They may be monitored or retrieved by supervision and are subject to court subpoena. The transmission of material that contains obscene or disparaging language or graphics is strictly prohibited. Employees may use messaging capabilities for departmental business only and may be disciplined for violations of this directive.

6. SYSTEM SECURITY: To protect the integrity of the computer system, certain levels of security have been established by the Department's Technical Services division. Employees are given a level of access into the computer system based on their job requirements. Employees shall not attempt to bypass, enhance, or otherwise modify the level of security they have been given.

A. It shall be the responsibility of the employee to protect the security of their assigned equipment and their system passwords. At no time shall an employee use another employee's password to access the computer system.

B. A two-factor authentication card will be issued to all personnel. This card must be used when accessing a tablet/laptop computer with ACJIC/NCIC access. When not in use, the card should be secured by its assigned user.

C. Tablet/laptop computers shall be properly locked in a computer mount when used in a police vehicle. When the employee is not on duty, and the vehicle is parked at their precinct or at their residence, the computer will be locked in the computer mount or removed from the vehicle and taken to a secure location. The security of the computer is the sole responsibility of the assigned employee.

D. The use of the tablet/laptop computer in conjunction with the police radio system is subject to the same restrictions placed on radio traffic. All messages and digital transmissions are subject to review.

7. NCIC/ACJIS SECURITY: The data accessed using the NCIC/ACJIS system must be protected to ensure correct, legal, and efficient dissemination and use. Personnel must follow proper procedures to make the information secure from any unauthorized access or use. Prior to accessing NCIC/ACJIS, authorized personnel must attend and successfully pass the MDT NCIC Course required by the Alabama Law Enforcement Agency (ALEA).

    A. The departmental tablet/laptop will have a direct link to the NCIC/ACJIS system. This system is password protected and allows authorized personnel to access classified records. The protection of passwords and the security of tablets/laptops are critical to prevent unauthorized access to NCIC/ACJIS data.

    B. The NCIC/ACJIS system is to be used for law enforcement purposes only and is not to be used in violation of the 1972 Federal Privacy Act regarding the dissemination of criminal records to unauthorized personnel. Personnel operating tablet/laptop computers will be held accountable for the protection of their respective passwords while accessing the system. Only authorized law enforcement personnel, while in the performance of their duties, are allowed access to the content(s) of any file retrievable through the computer.

    C. Any access to NCIC/ACJIS from a tablet/laptop computer is the responsibility of the employee whose password was used to log into the computer. Any employee who allows unauthorized access, whether willfully or through negligence, is subject to disciplinary action and possible criminal prosecution. If an employee is using the tablet/laptop computer to access NCIC/ACJIS and a civilian or unauthorized person is in the vehicle, the employee must ensure that the information on the computer screen is not visible to the unauthorized person. This may be accomplished by repositioning the computer screen or directing the unauthorized person to leave the immediate area of the vehicle.

    D. Information from NCIC/ACJIS must be kept strictly confidential. Under no circumstances will any employee use another employee's password to gain access to the NCIC/ACJIS system. Under no circumstances will any employee use a tablet/laptop that is logged on by another employee to access NCIC/ACJIS.

8. NCIC/ACJIS HIT CONFIRMATION: A NCIC/ACJIS hit advises the officer that a stolen report, missing person report, or arrest warrant has been filed. It also provides the date of theft, date missing, or date of warrant issue, which are matters to be considered by the receiving officer in arriving at an arrest decision. A hit is one fact which must be added to other facts by the officer in arriving at sufficient legal grounds for probable cause to arrest.

    A. When an officer receives a positive response from NCIC/ACJIS and an individual is being detained, or a piece of property may be seized, an immediate confirmation with the agency that originated the record in the system is necessary to ensure the validity of the hit before an arrest or seizure may be made. To confirm a hit means to verify with the entering agency that the missing person report, theft, or warrant is still outstanding and that the person or property inquired upon is identical to the person or property listed in the wanted person, missing person, or stolen property record.

    B. To initiate a hit confirmation, the officer must notify police records and give the exact information that was entered on the tablet/laptop computer to generate the original hit. The records personnel will then resubmit the inquiry using the data supplied by the officer in

the field. When the hit is received in records, the operator will then contact the entering agency and verify the hit. Any further information received by the Records Division will be relayed to the officer in the field. The officer can then use the verified information to establish sufficient grounds for probable cause to arrest and/or seize property.