ELIZABETH POLICE DEPARTMENT
GENERAL ORDERS

VOLUME: 5	CHAPTER: 22	# OF PAGES: 5

SUBJECT: MOBILE DATA TERMINALS (MDT'S)

EFFECTIVE DATE: **September 3, 2024**	ACCREDITATION STANDARDS: NJSACOP 3.5.6
BY THE ORDER OF: CHIEF GIACOMO SACCA	
BY AUTHORITY OF: POLICE DIRECTOR EARL J. GRAVES	
SUPERSEDES ORDER #:	

PURPOSE: The purpose of this policy is to describe the responsibilities of the agency pursuant to the Criminal Justice Information Security (CJIS) Agreement and the security of Mobile Data Terminal systems (MDT's) utilized by the police department.

POLICY: The police department will adhere to all internal and external security policies and CJIS agreements concerning MDT's.

PROCEDURE:

I. CJIS SECURITY AGREEMENT

A. The New Jersey State Police is considered a CJIS System Agency (CSA) responsible for administering the CJIS system at the local level.

B. The police department is considered the Criminal Justice Agency (CJA).

C. The use and access to MDT's in governed by the signed Criminal Justice Information Services (CJIS) Agreement between the police department (CJA) and the New Jersey State Police (CSA).

D. The police department (CJA) is committed to adhering to the CJIS Agreement or face possible CJIS sanctions by the New Jersey State Police (CSA).

II. MDT TRAINING

A. The police department Terminal Agency Coordinator (TAC) is responsible for training users in the appropriate level of access for the MDT use.

B. The TAC is responsible for maintaining all such training requirements consistent with the CJIS Agreement.

C. All such training records will be subject to an audit by the New Jersey State Police (CSA).

III. PASSWORDS

A. Passwords must be selected that are a minimum of 8 characters.

B. Passwords shall not be a dictionary word or proper name.

C. Passwords shall not be the same as the User ID.

D. Passwords shall expire within a maximum of 90 calendar days.

E. Passwords shall not be identical to the previous ten (10) passwords.

F. Passwords shall not be displayed when entered.

IV. MDT COMPUTER SECURITY

A. No user shall introduce, modify, or alter MDT software or related hardware. Any such action may jeopardize system security.

B. Officers utilizing MDT's must ensure that CJIS information displayed on the MDT is not visible to the public. Barring exigent circumstances, all windows on the MDT should be minimized when officers exit their vehicle. All MDT's when not in use shall be stored securely in a locked docking station.

C. All MDT data obtained via the MDT containing CJIS information shall be retained for a minimum of 1 year.

D. All information received via MDTs shall remain confidential. This includes but is not limited to information received through the NJCJIS system (NCIC, NLETS, NJLETS, MVC, AOCTELE (i.e. ACS, ATS, D.V.C.R. etc.)

E. No user shall obtain information through the MDT system for any purpose other than official criminal justice purposes.

F. Every transaction, or communication, involving the MDT system is recorded into the system server memory and is discoverable for court purposes. All MDT users shall follow proper protocol when using the system for messages. The sending of offensive, profane, childish or otherwise improper messages will subject the sender to disciplinary action.

V. SYSTEM OPERATION

A. OFFICERS SHALL NOT OPERATE THE MDT WHILE PHYSICALLY DRIVING THE POLICE VEHICLE.

1. These actions are prohibited while the patrol vehicle is in motion and the driver / officer is the vehicle's only occupant and/or authorized MDT user. During these times, officers shall obtain the requested information via dispatch over the police radio. However, an officer may operate their MDT while operating their police vehicle when it is not currently in motion (e.g., stopped at a red light / stop sign; pulled over to the side of the road, etc.).

B. During cold weather, when the vehicle and the computer have not been used and are cold, officers should allow the vehicle to warm up prior to starting the computer in order to avoid damage.

C. Computers are sensitive electronic equipment. Officers should make efforts to prevent fluids, dirt, magnetic fields and other foreign material from contacting or being in the vicinity of the computer.

D. Officers are responsible to ensure that the computer is in good working order at the beginning of the shift. The computer should be inspected for damage, abuse, foreign material. Any damage noted should be documented in writing immediately to a supervisor

E. In order to prevent spillage or damage, the area around the computer is to be kept free of food, beverages, clipboards, paperclips, etc. Other electronic devices (radar, microphone, pager, etc.) shall not be placed on the computers.

F. At the completion of the shift officers will log off and shut down the computer using proper log off procedure.

VI. ACCESSING NJMVC

A. As per the New Jersey Supreme Court ruling in State V. Donis, effective June 1, 1999, full disclosure motor vehicle registration lookups, using the New Jersey Motor Vehicle Commission (NJMVC) database, are not permitted without reason to suspect wrongdoing. However, limited disclosure of information is allowable by a random look up utilizing the NJMVC database.

B. A random look-up is one in which the officer has no reason to look-up the registration, that is to say the look-up is not suspicious in nature.

1. In *Donis,* the New Jersey Supreme Court placed a judicial check on random MDT searches conducted by police in New Jersey. The Court held it was permissible for police officers to run random MDT searches on license plates to determine if the vehicle was reported stolen or to verify the registration status of the vehicle or to verify the status of the registered owner's driver's license. However, the Court also held that is was not permissible for police officers to obtain the registered owner's personal information contained in NJMVC databases without "reason to suspect wrongdoing".

C. An officer may only access the full motor vehicle registration look-ups when he or she has articulable reasonable suspicion that the occupants are engaged in unlawful activity or the full motor vehicle registration look-up was reasonably related to an appropriate law enforcement purpose [N.J.S.A. 39:2-3.4(c)(1); e.g., a report of an unfamiliar vehicle parked in a residential neighborhood for a period of time]. The full motor vehicle registration look-up allows access to 'personal information" of the registered owner, including name, address, social security number, photograph, driver's license number, and if available, criminal record.

D. Reasonable suspicion that the occupants are engaged in unlawful activity includes suspicion of any and all criminal offenses, disorderly persons offenses, petty disorderly persons offenses, motor vehicle violations and town ordinance violations.

E. Officers conducting random look-ups with no articulable, reasonable suspicion must utilize NJMVC random transaction function.

1. MDT checks must not "be based on impermissible motives, such as race" (*St. v. Segars, 2002*). MDT checks will be constitutionally valid when initiated for no particular reason by a police officer on a vehicle operated on a roadway in front of him or her. MDT checks will be constitutionally invalid if there is "proof of a racial or class pattern to the police officer's selections." *(St. v. Myrick, 1995).*

F. Officers found to be using the NJMVC database, for random full motor vehicle registration lookups, without reason to suspect wrongdoing, will be subject to disciplinary action as well as civil action. Individuals are subject to criminal prosecution, departmental discipline, and/or civil liability for any unauthorized access to the C.J.I.S. system or unauthorized dissemination of C.J.I.S. material.

VII. HIT CONFIRMATION

A. When look-ups are entered, the MDT system queries multiple identifiers for the individual being checked, name, date of birth, social security number. A positive result or "hit" may be returned from NCIC on any one identifier match. Consequently, officers can expect to experience a large amount of "false" hits, positive responses that are not true matches.

B. An NCIC hit without further investigation is not probable cause to arrest an individual or seize property. It is one factor that should be added to the totality of the facts and circumstances for the officer to decide if there is probable cause to arrest or seize property.

C. An NCIC hit establishes reasonable suspicion to detain an individual to briefly investigate the circumstances and verify and confirm the NCIC hit. Whenever an officer receives a positive response (hit) from NCIC, the officer must confirm that the hit is for the person/vehicle/article that the officer has detained. Officers shall not arrest a person on an NCIC hit before confirming that the name and date of birth match, confirming that all other descriptive information matches, directing the dispatcher to confirm the validity of the NCIC hit with the originating agency.

D. The confirmation process will be according to current NJCJIS procedures.