ELIZABETH POLICE DEPARTMENT
GENERAL ORDERS

VOLUME: 5	CHAPTER: 22	# OF PAGES: 3

SUBJECT: MOBILE DATA TERMINALS (MDT'S)

EFFECTIVE DATE: **October 28, 2020**	ACCREDITATION STANDARDS: 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 UserID.

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. MDT's are considered portable devices; therefore, the device must maintain Advanced Authentication in order for a user to access the MDT.

1. The intent of Advanced Authentication is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

2. The police department TAC is responsible for assuring that all MDT's are configured for two-factor authentication consistent with the police department CJIS Agreement and the FBI Criminal Justice Information Security Policy August 2014.

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

C. All MDT's when not in use shall be stored securely in a locked vehicle or securely in police headquarters.

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