Subject: Use of MDTs	**Page 1 of 4**
Effective Date: August 2003	**Revision Date: September 2019**
Amends/Supercedes:1200.20 / August 2003	**Approved by: Chief Kevin Higdon**
Meets Accreditation Standard:	

Section 900.30 Use of Mobile Data Terminals

Policy

It is the policy of the Shively Police Department to implement mobile data terminals to assist officers in quickly accessing data and to provide the technological tools to make policing more efficient and modern.

The Shively Police Department will develop procedures that are approved by the Kentucky State Police that apply to security and operation of the records system.

All officers shall be in compliance with this policy when using:

Law Information Network of Kentucky (LINK)
National Law Enforcement Teletype System (NLETS)
National Crime and Information Center (NCIC)

This policy will address the following areas:

- **Passwords**
- **Logging**
- **Security/Confidentiality**
- **Records Management**
- **Dial up/Remote Access**
- **Use of Hit Terminal**

Passwords

With Mobile Data Terminals, certain pieces of information must be provided to begin operations of the system. Usernames and passwords are used to accomplish the logging on to database computer that is managed by the Kentucky State Police.

Usernames- The Shively Police Department will assign user names.
Passwords- Each individual officer authorized to use the system will choose a password that will be easy to remember. This password should be kept confidential.

- MDT operators are required to enter and maintain their own passwords.
- Password must be changed every sixty, (60) days, but may not be changed more often than every ten, (10) days.
- Each password must be at a minimum of five, (5) characters in length.

Logging

Officers may use the logging feature of the system. By recalling records from the log, officers could obtain an exact copy of the record as it was shown when it was initially run in the inquiry. This feature is helpful to officers for courtroom documentation.

The system log is maintained for a minimum of one (1) year.

Security/Confidentiality

Security of the system is of a major concern and it shall be the responsibility of every employee that is authorized to use the system to maintain the utmost respect for its content.

- No employee shall use the system for his or her own personal use or for the advancement of off duty endeavors.
- Employees shall keep official information confidential and only revealed as necessary in accordance to established police standards and practices.
- No employee shall tamper with the MDT in any way by adding or deleting software or adding or deleting hardware.
- No employee shall use the MDT for entertainment purposes such as gaming, social networking or viewing of videos unless authorized by the department.
- Employees should keep in mind that items that are on the MDT screen may be visible to citizens both inside and outside of the vehicle. Employees are prohibited from displaying images that may be offensive to persons of any gender, race, creed, color, ethnicity, sexual orientation, religious affiliation or political affiliation.
- Employees shall immediately report damage or problems with MDT’s to their immediate supervisors.
- Supervisors shall immediately document and report damage or problems with MDT’s to the Chief of police or Deputy Chief of Police.
- Employees found to be tampering with computers or violating the Kentucky State Police user agreement on the LINK/NCIC system may be subject to

    - Criminal prosecution
    - Civil prosecution
    - Subject to violation of this policy and others.

Records Management

Data systems produce large amounts of information and each system must have some type of record management/system administration in place. The Deputy Chief of Police, TAC officer or some other employee may be appointed by the Chief of Police to be the system administrator.

The Shively Police Department shall be responsible for the administrative function and shall not be delegated to a non-criminal justice third party (i.e. commercial vendor). Administrative functions include:

- Managing usernames and system rights
- Maintaining proper system configurations
- Enabling and disabling system features
- Recording and unloading archival files

All LINK transactions shall be logged electronically. The log shall include the following:

- Transaction requested
- Date and Time
- Operator terminal device
- Agency ORI using the MDT

Electronic logs shall be maintained for one (1) year.

Kentucky computerized criminal history access is not provided over the MDT system and attempts to access this type of information via the MDT system is **PROHIBITED.**

Dial Up/Remote Access

Remote dial up, Intranet or Internet access is strictly forbidden. The only exception to this policy is the vendor may use PCAnywhere (or similarly approved software) to dial into MDT controller to perform troubleshooting, software maintenance, or software upgrades.

Biological firewall – A biological firewall must be maintained at all times. This means that when the MDT is not in use it must not be capable of connectivity to a local area network, Intranet or the Internet.

Use of A Hit Terminal

The current LINK/NCIC terminal will be used as the designated MDT "hit terminal". The terminal is located in the Dispatch Center and will be used to print out a copy of any "hits" received by a MDT. This practice will help ensure officer safety, by allowing the dispatcher to be notified of any potential danger as soon as the hit response is returned.

Any member utilizing the MDT must be NCIC certified. When accessing the NCIC, the MDT must be inside of the vehicle. When the NCIC is accessed on a MDT in a departmental vehicle, the MDT screen shall be positioned so that it is out of the view of any passengers. The NCIC shall not be left visible on the screen when the MDT is not in use.

The NCIC shall only be accessed:

- On secured MDTs that are docked in a departmental vehicle; or
- On departmental computers in an approved, secured area.

Any departmental laptop that is used to access the NCIC must have dual authentication (mobile messenger) installed for operation.

SPECIALIZED UNITS WITH NCIC TERMINALS

Specialized units having a NCIC terminal or NCIC access with criminal history privileges maintain a log and will include the following information for every request:

- Officer’s full name and code number
- Type of investigation and case number

In addition, the unit commanders will allow the SPD Terminal Agency Coordinator (TAC) to audit the terminal and all paperwork, upon request.

CONFIDENTIALITY REQUIREMENTS

Due to the sensitive nature of the information, members are prohibited from copying, pasting, or otherwise entering NCIC information from a NCIC Terminal, Mobile Data Terminal (MDT), or any other device into any other document, computer program, or other electronic system. However, the information may be summarized and included in case. Members are also prohibited from taking photographs/screen shots of criminal histories. The NCIC shall not be left visible on the screen when the computer is not in use.

Criminal histories shall not be placed in a case file or given to anyone outside of the department. Criminal histories shall not be copied by any means (e.g. photocopied, scanned). Officers may record any pertinent information from a criminal history and include this information in an investigative letter. All criminal histories are to be shredded after the necessary information has been recorded.