

**EFFECTIVE:** 1 December 2001  
1 December 2007

**REVISED:** 1 December 2008  
1 January 2010  
20 June 2011

**SUBJECT:** Use and Security of the Mobile Data Computer (MDC)

**ISSUED BY:** Fernando Solorzano

**I. PURPOSE:**

To establish policy and procedural guidelines for use of the Mobile Data Computer (MDC) and the define Dispatcher and Field Unit responsibilities.

**II. POLICY:**

- (a) The MDC provides direct access to the Police Department's Computer Aided Dispatch and records management systems (VISION), and State and National Justice Database Systems. Security is of the utmost importance. Officers shall comply with all federal and state rules and regulations that apply.
- (b) The MDC system shall only be used by authorized employees.
- (c) The Chief of Police will designate a person(s) to act as the MDC Systems Coordinator(s). Terminals shall not be installed, removed, moved, or modified in any manner by anyone other than System Coordinator or Technical Service Personnel.
- (d) All MDC transmissions are recorded and subject to audit by the Police Department at any time without notice. The MDC shall not be used to transmit any message of a defamatory, racist, or sexual nature. Personnel shall not use the MDC to transmit messages that would reflect negatively upon the Police Department if examined under court subpoena. There are no expectations, or right of privacy while using a mobile data computer.
- (e) Field personnel shall use the MDC for receiving and acknowledging routine dispatch assignments, updating unit status, and querying databases when practical to do so, with due regard to officer safety.

- (f) Any status change or acknowledgement that is broadcast by voice, by a field unit, shall be entered into the CAD system only by the Dispatcher in order to avoid errors and duplication of effort.
- (g) Field personnel signed onto an MDC shall be responsible for monitoring the terminal and maintaining correct unit status on the CAD system.
  - (1) Any field unit in the available or enroute status is presumed to be in the unit and monitoring the MDC for assignments and messages.
  - (2) When away from the unit and not monitoring the MDC, field personnel shall change their status accordingly using the appropriate CAD call type and/or sub status code. If it is not practical to make this change on the MDC, voice notification must be made.

### III. SECURITY:

- (a) MDC passwords shall only be issued to employees upon approval of the Chief of Police and after completion of Department approved training. Personnel shall not reveal their individual password to another person.
- (b) Personnel shall only log onto the MDC using their own individual password.
- (c) Except as authorized below, personnel shall not use an MDC if another person has already logged onto it. Exceptions are as follows:
  - (1) Emergency situations requiring immediate access to information through the closest MDC
  - (2) Situations where multiple employees are assigned to share the same vehicle/MDC and the employee logged on is aware of its use
  - (3) Situations where multiple employees are assigned to the same incident and the employee logged on is aware of its use
  - (4) Authorized testing, maintenance or repair of the MDC
  - (5) When specifically authorized by the Watch Commander or Field Supervisor

### IV. PROCEDURE:

The MDC shall be used whenever practical, in order to reduce radio traffic. Obvious officer safety or urgent information will continue to be broadcast via voice transmission. Common sense and good judgment shall be used when deciding what should be voice vs. what should be sent via MDC. The field unit has the ultimate decision over when they will transition to voice broadcasts as situations in the field change.

### V. USE OF MDC WHILE OPERATING A VEHICLE:

Use of the MDC should be limited to times when the vehicle is stopped. Sending or reading MDC messages while a patrol vehicle is in motion is a potentially

dangerous practice. When the vehicle is in motion, officers may use a one stroke keys (i.e. en route, 10-97, display incident, etc.) generally located on the MDC screen. Also, simple transmissions, such as entry of a license for a 10-28/29 may be permitted. Reading messages while in motion should only be attempted when the message requires the officer's immediate attention. In no case shall an officer attempt to send or review lengthy messages while the patrol vehicle is in motion. Officers shall be responsible for the safe operation of the patrol vehicle during any MDC communication.

The MDC should never be used when it presents an immediate danger to that person. (i.e. running wanted person checks of driver's license status when no back-up officer is present)

**VI. LOG ON AND UNIT INFORMATION:**

When logging onto the MDC at the beginning of the officer's shift, field personnel are responsible for entering employee numbers, vehicle numbers, HT numbers and all supplement equipment information that is relative to the assignment (i.e. shotgun number).

**VII. HIGH PRIORITY INCIDENTS:**

Incidents of a high priority (i.e. priority 1, in progress priority 2, or priority 2 incidents occurring within 10 minutes containing suspect information) will be dispatched in the following format:

- (a) Field units will remain in a voice mode while responding and during the call until it is deemed "Code 4". Dispatchers will also remain in voice mode but will also send the call to the responding unit's MDC.
- (b) The dispatcher will verbally broadcast any critical supplements and changes to the call while units are enroute. The MDCs do not receive updated information. Any information that may need to be updated shall be done via voice broadcast.
- (c) Any status change of self-initiate given verbally by a field unit will be the dispatcher's responsibility to update.

**VIII. LOW PRIORITY INCIDENTS:**

Incidents of low priority should not be of felony in-progress or just occurred events. Those types of calls should be dispatched in a high priority format.

Examples of low priority calls are priority 2 not-in-progress or occurring within 10 minutes with no suspect information, and priority 3 and below. These calls will be dispatched in the following format:

- (a) Dispatch will utilize an abbreviated voice broadcast and send the call to the responding unit(s)' MDC.
- (b) The abbreviated broadcast will include the unit(s) assigned, type of call, location, and any special concerns. This broadcast is for the benefit of other field units and supervisors.
- (c) The responding unit(s) are responsible for all status changes and updates via the MDC (i.e. enroute or on scene and closure of the call) unless it would jeopardize the unit's safety.
- (d) Low priority calls will not require voice broadcasts by field personnel with MDCs unless more than one unit is assigned to the same call, then each unit shall advise on scene or other pertinent information via radio.
- (e) If the field unit assigned a call via MDC does not acknowledge the call by voice or by pressing the enroute button within a one minute period of time, dispatch shall contact the unit via radio and inform the officer to copy their MDC for information on the call.

#### IX. STOLEN VEHICLE/WANTED PERSONS:

If a field unit runs a vehicle license plate via the MDC and it returns as a reported stolen vehicle, dispatch will automatically be notified of the hit. The dispatcher will then verbally contact the field unit and confirm its status and location.

Hits on wanted persons are not automatically sent to dispatch. If a field unit reveals a subject is possibly wanted, the unit shall immediately notify dispatch verbally of the possible hit and request it be confirmed.

#### X. SAFETY CHECKS:

All safety checks of field personnel will be done via radio broadcast.

#### XI. CHANGING UNIT LOCATION/STATUS:

- (a) Field units will use the MDC to change locations whenever practical. If the unit chooses to verbally broadcast the update, the dispatcher will be responsible for changing the unit's status and its activity will be recorded by the dispatcher.
- (b) Field units will not dispatch themselves to pending calls. The unit shall request dispatch send them the call.

(c) Units will request and change their status to Code 7 via voice broadcast. The unit may use the MDC to change his/her status to 10-8 after completion of Code 7.

(d) Units will not place themselves unavailable without Supervisor approval.

**XII. CANCELLATIONS:**

(a) Any cancellation of unit response to a call by dispatch shall be broadcast and acknowledged verbally.

(b) Field units will be responsible for a verbal broadcast of Code 4 and/or the cancellation of other units responding when no further assistance is needed.

(c) When pre-empting a unit from a currently assigned call, the dispatcher shall verbally broadcast the cancellation of the first call prior to assigning the new call.

**XIII. ADDRESS AND PERSONAL HISTORY:**

Officer safety information pertinent to the call the officer(s) is enroute to shall be provided via voice broadcast and acknowledged verbally by the officer.

**XIV. BOMB CALLS:**

When investigating reports of possible bombs, officers will turn off their MDCs. This will be done to enhance officer safety at the scene. Operating the MDC may cause some devices to detonate, thus, all radio equipment should be turned off. It is the field unit's responsibility to advise dispatch that it will be operating off the air. If the field unit advising off the air is logged onto an MDC, dispatch shall automatically note the unit has shut off the MDC.

**XV. CLEARING INCIDENTS:**

(a) Units will have to contact dispatch to either verify or change the incident's location of occurrence.

(b) The assigned or handling unit will assign the file and clear the incident with a valid disposition code and correct heading.

**XVI. LOG OFF:**

(a) The field unit shall advise 10-7 via radio broadcast at his/her end of watch.

(b) It is the field unit's responsibility to properly log off the MDC at the end of watch by using the Log Off command.

- (c) The MDC should not be logged off or turned off during the shift, except as authorized. (e.g. Bomb Calls)
- (d) The MDC may be disabled for security reasons as needed by using the suspend function. To reactivate the MDC, again use the suspend function.

## XVII. AUDITS

- (a) The MDC Systems Coordinator will make periodic audits of the MDC Logs.
  - (1) The audit will include an examination of system transmissions to verify that policy regarding MDC use is being followed. These audits are not intended to be exhaustive, but rather will include a large enough sampling to predict overall compliance.
  - (2) Any transmission(s) found to be out of compliance with this policy shall be fully investigated.
  - (3) At a minimum these audits are to be conducted four times per year.

APPROVED