

IDAHO STATE POLICE PROCEDURE

07.06 MOBILE DATA COMPUTERS

I. GENERAL

Mobile Data Computers (MDC) use is in accordance with Idaho State Police (ISP) procedures [02.11 Use of Information Technology](#), [07.12 Patrol Radio Operations](#), and [11.01 ILETS Access Requirements](#).

II. DEFINITIONS

- A. “Mobile Data Computer (MDC)” means an electronic computer based system within a vehicle that provides direct access to national and local law enforcement databases and common computer functions governed by ISP procedures.

III. INSTALLATION AND CARE

- A. Public Safety Communications or its designee installs the mount and related equipment.
- B. Troopers may make minor adjustments to assist with equipment functionality, but are prohibited from moving the mount or making changes to the wiring.
- C. Troopers must ensure the MDC is secure in the mount prior to vehicle operation.
- D. Troopers may attach a USB keyboard and/or mouse.
- E. Troopers must clean the computer screen only with wipes manufactured for this specific purpose.
- F. Troopers must not affix any item using Velcro or a sticky backing to the computer screen or edges of the screen.
- G. All employees assigned MDC equipment and associated software applications must receive training on the use of MDC hardware and software prior to use.

IV. SECURITY

- A. All MDC's are protected using assigned password(s) and other security devices and protocols.
- B. Users must take reasonable steps to ensure unauthorized persons and vehicle occupants do not view displayed data or hear audio returns.
- C. Users must take reasonable steps to ensure protection against unauthorized use of the MDC by closing the screen, logging off, or locking the MDC when leaving the vehicle for an extended period.
- D. In case of a damaged, lost, or stolen MDC, users must:
 - 1. Immediately notify a supervisor for completion of appropriate paperwork;
 - 2. Ensure the MDC ID is entered into NCIC stolen article files;

IDAHO STATE POLICE PROCEDURE

3. Notify ITS; and
4. Ensure any data stored on the MDC prior to damage or loss has been forwarded to the appropriate court.

V. TYLER TECHNOLOGIES

- A. All users who have access to NCIC restricted data will remain certified in conjunction with [11.01 ILETS Access](#) Requirements
- B. Traffic stops, motorist assists, physical checks on suspicious vehicles or suspicious persons are initiated by radio; additional information may be obtained either by MDC or by voice communication.
- C. For all contacts, troopers must advise of the contact's name and DOB prior to clearing the stop either by voice communication or MDC.
- D. When a trooper runs a driver check using an MDC and the subject returns with a misdemeanor or felony warrant or other actionable NCIC hit, the trooper immediately notifies dispatch. Dispatch will handle according to [ISP Policy 7.12 Patrol Radio Operations](#).

VI. SPECIAL CONSIDERATIONS

- A. Use of the MDC by the trooper should be limited to times when the vehicle is stopped.
- B. Short data entry such as entry of a license number for a stolen or registration check are permitted if they can be done safely.
- C. Reading messages while in motion by the trooper should only be attempted when the message requires the trooper's immediate attention, and the action can be done safely.
- D. In no case shall the trooper attempt to send or review any message that would compromise the safe operation of the vehicle, while the vehicle is in motion. Focusing attention on the operation of the MDC must not detract from the safe and responsible operation of the vehicle.
- E. Only ISP approved software may be installed on MDC's. Employees must not install unauthorized programs or media.
- F. Records of MDC usage may be reviewed by supervisors at any time without prior notification or permission.
- G. Troopers using the MDC must comply with all applicable federal and state rules and regulations.