ILLINOIS STATE POLICE DIRECTIVE
SRV-208, MOBILE DATA COMPUTER SYSTEMS

RESCINDS: SRV-208, 2012-053, revised 06-10-2013.	**REVISED:** 10-02-2014 **2014-074**
RELATED DOCUMENTS: ADM-128, EQP-013, SRV-200, SRV-202, SRV-204, SRV-218	**RELATED CALEA STANDARDS:** 11.4.4, 41.3.7, 81.2.9, 82.1.1

I. POLICY

The Illinois State Police (ISP) will establish guidelines and rules governing the safe use of mobile data computer systems in ISP vehicles.

II. DEFINITIONS

II.A. Illinois Wireless Information Network (IWIN)

II.A.1. IWIN is a wireless mobile data network for interested state and local Illinois government agencies that provides access to the following, including, but not limited to:

II.A.1.a. Law Enforcement Agencies Data System (LEADS)
II.A.1.b. National Crime Information Center (NCIC)
II.A.1.c. Secretary of State (SOS)
II.A.1.d. The International Justice and Public Safety Network (Nlets)
II.A.1.e. Criminal History Record Information (CHRI)

II.A.2. IWIN uses mobile data computers to send and receive encrypted and compressed data (LEADS, CHRI, IWIN messaging).

II.A.3. The Illinois Department of Central Management Services (CMS) manages and supports IWIN.

II.B. IWIN Administrator - the individual who coordinates the IWIN program within ISP and manages the IWIN Project Team.

II.C. IWIN Coordinator - the individual, assigned to a group of IWIN users, who is responsible for overseeing the certification, activation, and primary support for their IWIN users. The IWIN Coordinator serves as the liaison between the IWIN Project Team and the field, as well as notifying the coordinator's command staff and their IWIN users of issues, updates, and/or problems with IWIN. (See the IWIN Procedural Manual for details on the IWIN Coordinator's responsibilities.)

II.D. Mobile Data Computer (MDC) - a laptop version of a personal computer that can be used by field staff to obtain wireless mobile access to external data sources.

II.E. MDC System - the following equipment comprises a complete MDC system:

II.E.1. MDC (includes integrated cellular wireless modem and carrying case)

II.E.2. In-car printer

II.E.3. Dual band cellular wireless antenna

II.E.4. Docking and mounting hardware

II.E.5. Software

III. PROCEDURES

III.A. IWIN users should refer to the IWIN Procedures Manual for detailed procedures governing the use of IWIN.

III.A.1. The IWIN Procedures Manual is located on the IWIN Intranet Site (http://home/itc/iwin/html/iwinhome.htm).

III.A.2. Users should periodically review the IWIN Intranet for updates to the IWIN Procedures Manual.

III.B. Assignment, security, and storage of equipment

III.B.1. Assignment of equipment

III.B.1.a. IWIN equipment will be issued/assigned to individuals following the procedures in ISP directive ADM-128, "Property Control."

III.B.1.b. Individuals are responsible for the care and security of each piece of equipment assigned to them or to their assigned vehicle.

III.B.1.c. Individuals are accountable for issued IWIN equipment and will obtain written receipt for any item returned or exchanged. (See ISP directive EQP-013, “Return of State Owned Items of Issue.”)

III.B.2. End-of-shift removal and storage of equipment

III.B.2.a. Following his/her shift, if the user’s vehicle will be secured in a locked garage, all IWIN equipment MAY remain in the vehicle.

III.B.2.b. If a user’s vehicle is NOT secured in a locked garage, the officer will remove the MDC from the vehicle and store it in his/her residence or locked office.

III.B.3. On-duty storage

When a vehicle mount is provided, and while the user is on duty, the MDC will be mounted in the authorized docking device in the vehicle.

III.B.3.a. When a vehicle mount is not provided, the user will ensure the MDC is secured in a location so as to reduce the risk of damage to the MDC while the vehicle is in use. The MDC will be secured and/or stored in a location so as not to impede the driver or interfere with the safe operation of the vehicle while the vehicle is in use.

III.B.4. Unattended vehicles

III.B.4.a. Users will lock vehicles when left unattended.

III.B.4.b. Users will use every precaution to safeguard equipment when the equipment is not in their immediate possession.

III.B.4.b.1) Users will remove, if necessary, the MDC from the vehicle.

III.B.4.b.2) Any MDC left in an unattended vehicle must be locked in the dock with the dock key removed from the vehicle (when a dock is provided). If a dock is not provided, the MDC will be placed in its carrying case and locked in the trunk, if weather conditions permit. If the vehicle does not have a trunk, the MDC will be stored under the rear seat, inside the large console, etc., so long as it remains out of sight. If the vehicle were to remain unattended for an extended period of time then the MDC should be stored at the officer’s residence.

III.B.4.c. The MDC will not be secured in any location that exposes the MDC to extreme heat or cold.

III.B.4.d. Users will log off IWIN if the computer is being left unattended.

III.B.4.e. In sub-freezing temperatures, to reduce the MDC's warm-up time, consideration will be given to removing the MDC from the vehicle if the user will be out of the vehicle for an extended period. However, the security of the MDC when removed from the vehicle will be the primary deciding factor.

III.B.5. Stolen or damaged IWIN equipment

III.B.5.a. Users will immediately notify the ISP Integrated Technical Help Desk in Springfield, 217/782-4155 or 866/532-3700, if it is believed an MDC (or the vehicle with the MDC in it) was stolen. The Integrated Technical Help Desk will contact the CMS Support Center and a member of the IWIN Team who will take steps to deactivate the Internet Provider (IP) address.

III.B.5.b. Personnel assigned MDC equipment are responsible for any stolen, missing, or damaged item if the vehicle is left unlocked when unattended or otherwise not secured in accordance with policy.

III.B.5.c. Sworn officers will complete an ICase report when IWIN equipment is lost, stolen, or damaged while in the custody of the sworn officer.

III.B.5.d. Code personnel will complete a memorandum detailing the particulars of the loss when IWIN equipment is lost, stolen or damaged while in the custody of the code employee.

III.B.6. Passwords

III.B.6.a. Users will not give their passwords to any person to use nor will they leave the password in any discernible written form on or near the computer.

III.B.6.b. If an emergency requires a user to share a userid and password with another person, the user sharing the password has full responsibility for the use of the MDC system by the person with whom the userid and password have been shared. At the earliest possible time, the user will change or cause his/her password to be changed.

III.B.6.c. Users will follow password procedures in ISP directive SRV-218, “Password Control,” except if a user forgets his/her Premier MDC password. Then, the user must contact CMS Customer Service Center at 800/366-8768, Option 4, then Option 1.

III.C. Restrictions regarding IWIN access

III.C.1. Users will:

III.C.1.a. Restrict dissemination of information received through IWIN to criminal justice personnel in the furtherance of their official duties.

III.C.1.b. Perform transactions for criminal justice purposes only.

III.C.1.c. Follow data access and information security procedures outlined in ISP directive SRV-200 "Information Security and Disposal of Personal Information."

III.C.2. Users WILL NOT:

III.C.2.a. Access criminal history files, except as provided for by law.

III.C.2.b. Access database records for any reason other than legitimate law enforcement purposes.

III.C.2.c. Permit use of the LEADS material by any individual who is not certified for LEADS access.

III.D. Authorized/unauthorized use

III.D.1. Use of the MDC is restricted to official ISP business. Computer files, web browsing history, all messaging, software installed, and LEADS inquiries, are subject to review without notice to the user. There is no expectation of privacy with respect to use of the MDC.

III.D.1.a. To obtain LEADS inquiry logs or messaging logs made via IWIN, the requester must complete the "ISP Request to CMS for IWIN User Data," form ISP 9-30 (this form is available in the ISP Document Library at http://maphome/documentlibrary/ and also on the ISP and IWIN Intranet (F8) accessed via IWIN).

III.D.1.b. This request requires signature approval by either the Bureau Chief or the Zone/District/Regional Commander of the requesting unit. Upon approval, fax, scan and email, or mail the request form to:

IWIN Administrator
801 South Seventh Street, Suite 400N
Springfield, Illinois 62794-9641
Fax: 217/557-1262

III.D.1.c. LEADS inquiry logs or messaging logs made via IWIN may not be disseminated outside of ISP without approval from the IWIN Administrator.

III.D.2. Use of the MDC by anyone other than authorized department employees requires written authorization via email or memorandum from the District/Unit Commander.

III.D.3. Users are responsible for ensuring the security of the computer against unauthorized use.

III.D.4. Immediately notify the Integrated Technical Help Desk in Springfield at the telephone numbers listed in paragraph III.B.5.a. if it is believed unauthorized access was attempted or has occurred. The Integrated Technical Help Desk will contact CMS and a member of the IWIN Team who will take steps to deactivate the IP address.

III.D.5. Users who are going to be leaving the continental United States and who require use of the MDC for official ISP business will make a request through the chain-of-command to the Colonel. If approved, the Colonel will forward the request to the Telecommunications Section, Logistics Bureau, DOA, who will obtain data roaming services for the MDC while the employee is out of the country.

III.E. Software restrictions

III.E.1. ISP directive SRV-204, "Local Area Network (LAN) and Wide Area Network (WAN) Access and Administration," regarding department personal computers and software are applicable to MDCs.

III.E.2. If an IWIN user wants to load any additional software on his/her MDC, he/she must send a written request to the IWIN Coordinator through the user's supervisor. The IWIN Coordinator will submit the request to the IWIN Administrator in Springfield or send the request over e-mail to IWINADM for consideration.

III.E.3. Any unauthorized software found on ISP MDCs during maintenance work, upgrades, or inspections, will be removed and the employee will be put on notice.

III.E.4. Users will **NOT** close the McAfee Anti-virus Program and will leave it running at ALL TIMES.

III.E.5. Automated security updates

III.E.5.a. All MDCs will be set for automatic updates from the web for Windows and anti-virus software.

III.E.5.b. If a user delays an automatic update, the user must complete the update as soon as time permits.

III.F. Operating an MDC while in the vehicle

III.F.1. Officers are encouraged to activate the text-to-voice module that increases officer safety by allowing the officer to hear the information sent from CAD, LEADS, or Messaging.

III.F.2. To ensure user and public safety, the driver should stop his/her vehicle and park in a safe manner before attempting to access information via keyboard. If it is necessary for the driver to access IWIN while the vehicle is in motion, the driver will exercise extreme caution to maintain driving awareness by keeping his/her eyes on the road and his/her surroundings and only glancing at the MDC monitor or keyboard for very brief intervals.

III.G. Hazardous operating areas

III.G.1. Due to potential effects of cellular transmissions from the cellular wireless modem, users will not operate IWIN in the following areas:

III.G.1.a. Within 500 feet of areas where blasting is in progress
III.G.1.b. Areas where explosive atmosphere exists, i.e., gasoline spills, etc.
III.G.1.c. Near medical or life support equipment
III.G.1.d. On an aircraft

III.G.2. In areas where cellular transmissions are potentially harmful, the user should turn off the power to the modem.

III.H. When MDC equipment malfunctions, refer to the IWIN procedures manual for instructions.

III.I. Training

III.I.1. IWIN Certification - All users must complete IWIN training through the Learning Management System (LMS) accessed through the ISP Internet at http://lms.ileas.isp.state.il.us.

III.I.2. LEADS Certification

III.I.2.a. All users who want access to LEADS via IWIN must minimally complete the LEADS Less than Full Access (LTFA) certification.
III.I.2.b. This course is available through the ISP Internet at http://lms.ileas.isp.state.il.us.

III.I.2.b.1) Users are responsible for printing out their certifications and providing a copy to their IWIN Coordinator.
III.I.2.b.2) LEADS recertification

III.I.2.b.2)a) LEADS users must renew their LEADS certification every two years prior to the expiration.
III.I.2.b.2)b) Users are eligible to take the LEADS Recertification CBT if their certificate is less than two years old.

III.I.2.b.3) Expired LEADS certification

III.I.2.b.3)a) A user's LEADS certification expires every two years.
III.I.2.b.3)b) If a user's LEADS certification is expired, LEADS access for that user via IWIN is terminated until LEADS certification is renewed.
III.I.2.b.3)c) If a user's LEADS certification is expired, the user will not be eligible to take the LEADS Recertification course and must pass the LEADS LTFA-Certification course.

III.I.3. Verification of Training

III.I.3.a. Users must print out the certificates demonstrating successful completion of these modules and provide them to the IWIN Coordinator.

III.I.3.b. The IWIN Coordinator will place a copy of the certificates in the user's training file.

III.J. Support Procedures

In the event a user encounters difficulties or problems associated with operating the MDC system, he/she will take the following steps in sequence to resolve the problem:

III.J.1. Refer to in-car trouble shooting tools to determine if there is a quick-fix solution.

III.J.2. Contact his/her IWIN Coordinator.

Indicates new or revised items.

-End of Directive-