



Illinois Statewide IWIN Policy Manual

IWIN Statewide Policies and Procedures

The following policies and procedures were developed to provide direction to all IWIN users statewide. Since IWIN provides users access to LEADS, particular emphasis is placed on restrictions regarding dissemination of LEADS information. Also, due to the ability to access LEADS through mobile data computers, emphasis is placed on the security of the equipment to eliminate unauthorized use. Throughout this policy manual, any reference to MDC (mobile data computer) will be synonymous with any computer used to access IWIN.

I. Responsibilities

Department of Central Management Services - IWIN Support Center

Responsibilities:

1. Administer the IWIN network/middleware server.
2. Maintain the 24-hour, 7-day per week IWIN Support Center for problems associated with the IWIN network
3. Contract with a mobile provider(s) for mobile coverage and enforce contractual obligations of the provider(s).
4. Assist all IWIN users in resolving problems related to:
 - a. Log on / log off procedures
 - b. Passwords
 - c. Messaging Module
 - d. Paging Module
 - e. Emergency Button
 - f. Mobile Network issues

Illinois State Police

Responsibilities:

1. Assist all IWIN users in resolving problems related to LEADS.
2. Audit IWIN agencies concerning the compliance with IWIN and LEADS rules, policy and procedures.
3. Maintain database of certified LEADS users for IWIN.
4. Administer Computer Based Training (CBT) program.
5. Maintain master list of ISP IWIN Coordinators and keep CMS informed of updates.

Local Agency IWIN Coordinator

Responsibilities:

1. Provide first-level trouble shooting and technical assistance to their agency's IWIN users and satellite servers.
2. Serve as the initial contact for all agency related trouble calls.
3. Receive and disperse any IWIN broadcast messages to the agency's IWIN users.
4. Coordinate the installation of all software and hardware.
5. Ensure that all required fields are completed on the Wireless Service Request (WSR) order form and all information is accurate and complete when submitted to IWIN.
6. Ensure that all agency mobile data users are aware of IWIN policies and procedures.
7. Ensure agency's IWIN users have their own IWIN user I.D. and only use it to access the IWIN system.
8. Attend all IWIN related informational sessions and meetings.
9. Assist users with accessing computer-based training modules.
10. Ensure all sensitive information which may be stored on the MDC is removed before equipment is sent in for warranty repair/replacement
11. Ensure all agency devices (including Satellite Servers) connected to IWIN have virus protection software installed with the latest definition files. The virus definition files can be acquired from the manufacturer of the virus protection software.

IWIN User

Responsibilities:

1. Unattended Vehicles:
 - a. Lock vehicles with IWIN equipment when the vehicle is left unattended.
 - b. Safeguard equipment when the equipment is not in their immediate possession or the vehicle is left unattended.
 - c. Log off of IWIN if the MDC is being left unattended.

2. Authorized/Unauthorized Use:
 - a. Restrict use of the MDC to authorized LEADS certified users.
 - b. Ensure the security of the computer against unauthorized use.
 - c. **Contact IWIN Support immediately at 800-366-8768 if it is believed unauthorized access was attempted or has occurred.**

3. Passwords:
 - a. Keep their passwords secret and not leave the password in any discernible written form in or near the computer.
 - b. If in an emergency it becomes necessary to share a user i.d. and password with another person, the person sharing the password has full responsibility for that person's usage of the system and at the earliest possible time should change his/her password.

4. Stolen Vehicles and/or MDC:
 - a. **Notify IWIN Support at 800-366-8768 immediately if it is believed an MDC (or the vehicle with the MDC in it) was stolen.**

5. **Restrictions regarding IWIN access:**
 - a. **Users shall restrict dissemination of information received through IWIN to authorized criminal justice persons only.**
 - b. **Users shall perform transactions for criminal justice purposes only.**
 - c. **Users SHALL NOT access criminal history files except as provided for by law.**
 - d. **Users SHALL NOT access database records for any reason other than legitimate law enforcement purposes.**
 - e. **Users SHALL NOT permit use of the MDC to access LEADS by any individual who is not certified for LEADS access.**
 - f. **Only mobile devices and State of Illinois frame network connected devices will be allowed on IWIN.**

6. Recommended policy for storage and security of IWIN equipment:
 - a. When a vehicle is not being used for duty, secure the vehicle in a locked garage, if the IWIN MDC remains in the vehicle. Otherwise, remove the IWIN computer from the vehicle and store it in the user's residence or locked garage.
 - b. When a vehicle mount is provided, ensure the IWIN computer is mounted in the authorized docking device in the vehicle while the user is on duty, unless the MDC is removed from the vehicle.

7. Recommended policy regarding operating an MDC/PDC while in the vehicle:
 - a. The driver of a vehicle should limit use of the MDC while the vehicle is in motion. When practical, the driver should stop their vehicle and park in a safe manner before attempting to access information.
 - b. Users are encouraged to activate the text-to-voice module which increases officer safety by allowing the officer to hear the information sent from the CAD, LEADS or Messaging.
 - c. If it is necessary for the driver to access IWIN while the vehicle is in motion, the driver should exercise caution to maintain driving awareness.

II. IWIN Training

LEADS Less-Than-Full Access Certification

LEADS/NCIC requires that anyone with direct access to LEADS be LEADS certified. The training includes inquiry, response interpretation, operational policies and procedures, and rules/regulations. There are several methods for obtaining this certification:

1. Internet (cbt.isp.state.il.us).
2. Computer Based Training accessed through a CBT server in an ISP district office or through frame relay connectivity to ISP. Please call the ISP LEADS Help Desk at 1-866LEADS00 (217-532-3700) for information regarding the CBT.
3. Classroom training provided by the ISP field specialists.

Computer-based Training Modules

1. IWIN Policies and Procedures - Each IWIN user will complete training on IWIN policies and procedures via CBT loaded on the MDC.
2. IWIN Hardware Training - CBT is available to local agencies purchasing the same IWIN equipment configuration as the ISP including the MDC, printer and bar code reader/imager.

III. Support Procedures

Step 1

Use Trouble Shooting Tools

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

- Automated Panasonic User Manual – Located on the MDC
- Motorola Premier MDC Software User Guide - Located on the IWIN Help Menu.
- Windows Help Menu - Look under "Trouble Shooting"

Step 2

Contact the Agency IWIN Coordinator for assistance in trouble-shooting

Step 3 - Network Related Support

Contact the IWIN Support Center at CMS for network-related problems or problems associated with logging on or accessing IWIN. Support is available 24-hours, seven-days a week.

IWIN Support Center – 800-366-8768

When calling the IWIN Support Center please have the following information available:

- IP Address, Cell channel, RSSI
- Exact geographical location where problem occurred
- The nature of the problem (exact error message)
- The steps that have been taken for problem resolution

Step 4 - LEADS Related Support

Contact the Illinois State Police Help Desk for issues related to LEADS.

Illinois State Police Help Desk - (217) 782-4155

IV. Motorola Client Functions

The Motorola Client features a graphical Windows interface to a variety of databases/applications. These applications can be activated by the keyboard, mouse or touch screen (if available) through the buttons located on

the client function bar at the top of the screen.

F1 Logon / Logoff

1. Users will enter the following:
 - a. Assigned User ID (4-8 characters)
 - b. Assigned User Password (4-8 characters)
 - c. Unit Number (1-6 positions)
2. Passwords:
 - a. The user may change passwords at any time.
 - b. Passwords should be kept confidential.
3. Logoff:
 - a. User should LOG OFF of IWIN through the F1 function at the end of their tour of duty or whenever leaving the vehicle for extended periods of time. Users who do not properly log off of IWIN before powering down the MDC, will remain logged on in the user registry.
 - b. Powering down the MDCs - Windows requires all applications to be shut down before powering off the MDC. Failure to close down applications, including the modem software and the Premier MDC may cause startup errors.

F2 CAD Computer Assisted Dispatch Module (where available)

F3 LEADS

1. IWIN users may have LEADS inquiry and messaging capability. Policies and procedures for LEADS are included in the Illinois LEADS Reference Manual.
2. LEADS Messaging Capability (See Messaging Module, for more detail):
 - a. Messages may be sent car-to-car and to any land-based LEADS terminal.
 - b. **Messages sent by users via LEADS should be limited to criminal justice or public safety purposes.**
 - c. All messages are logged.
3. Images:
 - a. IWIN will enable the ability to send and receive limited images over the IWIN network. **This functionality is restricted to criminal justice purposes.**
4. Criminal History Record Information (CHRI):
 - a. IWIN users are authorized to make CQH inquiries, which generates an inquiry to the Illinois Bureau of Identification and NCIC Interstate Identification Index (III).
 - b. All additional CHRI inquiries must be made through the communications center.
 - c. For additional details concerning CHRI, refer to the ISP Communications Policies and Procedures Manual, CHRI Chapter or the LEADS Reference Manual, CHRI chapter.
5. Each ISP district and local agency is assigned a separate CDC (Call Directing Code) for IWIN, which allows for communications between the MDCs and LEADS.

***Restrictions for all LEADS Messaging**

Criminal Justice Purposes Only

Messages sent by users should be limited to messages concerning criminal justice activities.

Personal Messages Are Prohibited:

- a. **It is strictly forbidden to transmit messages over LEADS for reasons of personal, unofficial communication.**
- b. **Message logging will be conducted by the Illinois Department of Central Management Services, and forwarded to IWIN Coordinators for review.**

Seminar, Training Class and Convention Announcements Prohibited:

- a. Such messages may not be transmitted through IWIN.
- b. Using LEADS to announce an event intended to make a profit is strictly prohibited.

F4 Message

Premier MDC enables messaging between the user and any other users or groups of users in the IWIN registry. All IWIN messages are logged.

1. Messages can be viewed and replies sent from the View Message Detail screen accessed through the MESSAGES button on the PMDC function bar.
2. Through the PMDC function, officers can send messages to any other IWIN user or ALERTS user.

F6 Paging Module

1. This module will allow users to page from their MDC anyone with a pager who has been entered into the system.
2. IWIN supports most numeric as well as alphanumeric pagers.
3. Users do not need to be logged on to IWIN to receive pages.
4. IWIN users will not be capable of sending a page to individuals who are not registered IWIN users.

F7 Mapping (for agencies purchasing the appropriate software)

1. In-vehicle mapping is available through the MAPPING button on the PMDC function bar.
2. Officers can zoom in and pan maps to more closely examine locations.
3. While the MDC is docked, the user's location will be tracked on the map within the mapping module on that user's MDC. (For agencies also having modems with GPS functionality)

F11 Emergency

A special button has been designed on the Premier MDC tool bar called "EMERGENCY".

1. "EMERGENCY" Key Purpose - Users should use the "EMERGENCY" button only when:
 - a. The user cannot get through on the radio (telecommunicator or another officer is transmitting) and the user has emergency (10-33) radio traffic; or
 - b. The user is unable to initiate voice communications and the officer needs to indicate he/she needs emergency assistance.
2. When a user activates the "EMERGENCY" button, a window appears which asks the user, "DO YOU NEED EMERGENCY ASSISTANCE?" The user has the option of selecting "YES", "CANCEL" or doing nothing. If the user clicks "YES", an emergency message is automatically sent back to the agency's communications center requesting emergency assistance. If the user selects "CANCEL", no request for emergency assistance will be sent. If the user selects neither the "YES" nor "CANCEL" buttons, the window will disappear after five seconds and no request for emergency assistance will be sent.

V. FCC Rules and Regulations

- | |
|---|
| <ol style="list-style-type: none"> 1. All MDC transmissions must comply with FCC rules and regulations. Only such calls as are specifically authorized by governing stations in the public safety services may be transmitted. 2. False calls, false or fraudulent distress signals, superfluous and unidentified communications, obscene, indecent, or profane language and the transmission of unassigned call signals are specifically prohibited. 3. Stations in the public safety service are primarily authorized to transmit communications directly relating to public safety, protection of life and property, and communications essential to official public safety |
|---|

activities.

VI. IWIN Reporting and Records Retention

1. Reports

IWIN reports can be obtained using two methods:

1. User agency can submit a Report Request Form signed by the Agency Director, Chief of Police, or Sheriff. This form can be found on the IWIN website www.state.il.us/iwin under 'Forms'.
2. User agency IWIN coordinators can log into the IWIN web based Reporting Server and run IWIN reports for their department. Coordinators wishing to do this should contact the IWIN Support Center at 800-366-8768.

2. Records Retention

Messaging and LEADS data will be kept available on the IWIN Reporting Server for one year. The data is then archived at the State Of Illinois.

VII. Satellite Server TCP Redirector

*** Note - Any department wanting to use TCP Redirector must use a Motorola Satellite Server for TCP Redirector applications. The application must also be reviewed, tested, and approved by CMS.**

1. **Redirector –E -Mail** allows the following TCP/IP, LAN-based client applications to communicate with their associated server over a Motorola-supported RF network:
 - a. Microsoft Outlook using the standard SMTP/POP3 protocols only
 - b. Microsoft Outlook Express using the standard SMTP/POP3 protocols only
 - c. GroupWise version 5.5 or greater using the standard SMTP/POP3 protocols only.

Redirector E-Mail is not intended for use with all applications, and some restrictions apply. For example, to reduce overloading the wireless network, the issue of e-mail attachment sizes should be carefully considered. Basic text messages are most suitable for Redirector E-Mail. Sending and receiving attachments is supported but not recommended due to bandwidth constraints. CMS requires a 20k attachment size limit for any attachments sent or received. It is the responsibility of the department to ensure this size limit is enforced.

2. **Redirector - Terminal Emulation** allows the following TCP/IP, LAN-based client applications to communicate with their associated server over a Motorola-supported wireless network:
 - a. IBM client access v3R1M3 (TN 3270/TN5250 only).
 - b. Seagull GUI/400 (TN3270/TN5250 only).
3. **Redirector-Web** enables an agency to wirelessly connect its mobile workstations to the agency's Intranet. Microsoft Internet Explorer web browsers can be configured to connect through Redirector-Web to the web server they normally connect to over a LAN. Redirector-Web acts as a bridge for wireless connection between the Internet web browser and the web server.

Redirector-Web supports standard HTML, XML-based web screens. Some web interfaces may not be supported or work optimally, such as advanced Java/Shockwave and other third-party applets.

Redirector-Web requires a proxy server with a static IP address.

- A. Redirector-Web has tested successfully with the following:
 - a. An embedded Microsoft Internet Explorer control.
 - b. Microsoft Internet Explorer versions 5.0 and 5.5.

VIII. Definitions

CBT - Computer-Based Training is a method of providing training to an individual using a software application that provides an instruction module(s) to a user via a computer. Many CBTs also include user interaction and can record a user's learning progress.

CDMA – Code Division Multiple Access

Computer - A device that calculates (processor) and retains calculations and data in a short-term memory bank (Random Access Memory, RAM) and stores data long-term (disk drive).

Desktop Software - A descriptive word referring to software which resides on the hard drive of a personal computer, for example, PMDC Client, Micro Soft Word, Micro Soft Excel, etc.

Illinois Wireless Information Network - IWIN is a wireless mobile data network available to state and local government agencies within Illinois that provides access to:

1. LEADS (Law Enforcement Agencies Data System);
2. NCIC (National Crime Information Center);
3. SOS (Secretary of State);
4. NLETS (National Law Enforcement Telecommunications System); and
5. CHRI (Criminal History Record Information).

IWIN utilizes mobile data computers with CDMA modems and Premier MDC software to send and receive encrypted and compressed data via CDMA equipped cellular towers and communications interfaces. IWIN is managed and supported by the Illinois Department of Central Management Services.

MDC System - The following equipment comprises a complete MDC system:

1. Mobile Data Computer
2. In-car Printer
3. Bar Code Reader/Imager
4. Modem
5. Docking and Mounting Hardware
6. Software

Mobile Data Computer - A laptop version of a personal computer capable of running off battery power alone. A mobile data terminal cannot perform calculations or store information, as a computer can.

Portable Data Computer - A version of a mobile data computer in which the keyboard may be detached from the display. The display operates through pen/touch services.

Peripheral Equipment - Any equipment that is attached to a computer system or computer dock (i.e. bar code scanners, printers, cameras, CD-ROM drives, etc.).

Premier MDC (PMDC) - The software developed by Motorola, which enables mobile users to access remote databases, to communicate with other users and to access other applications such as CAD or field-based mobile reporting.