University of CINCINNATI

Department of Public Safety
Police Division
Policies and Procedures

Title	SOP Number
RCIC/LEADS/NCIC Terminal Usage	16.2.400

Approval Signature
Eliot K. Isaac

Eliot K Isaac	

Reviewed/Revised by	Pages 6

Last Revision Date	Effective Date
October 31, 2024	May 6, 2015

RCIC/LEADS/NCIC Terminal Usage

I. **Purpose:** To provide University of Cincinnati Police Division (UCPD) personnel with guidelines for the proper use of the equipment and to ensure the proper dissemination of information and messages sent or received using an RCIC or MDC terminal.

II. **Policy:** It is the policy of UCPD to adhere to the national, state, and local standards regarding access to RCIC, LEADS, and NCIC information and to effectively utilize these systems for law enforcement activities.

III. **Definitions:**

RCIC – Regional Computer Information Center (RCIC is a regional computer network that provides computerized data and communication for criminal justice agencies within Hamilton County)

LEADS – Law Enforcement Automated Data System (LEADS is a statewide computer network that provides computerized data and communication for criminal justice agencies within the state of Ohio)

NCIC – National Crime Information Center (NCIC is a nationwide computer network that provides computerized data and communication for criminal justice agencies within the United States)

MDC – Mobile Data Computer

TAC – Terminal Agency Coordinator – an appointed member of the agency responsible for all aspects of day-to-day terminal operations and overall compliance with all rules and policies of LEADS and CJIS

IV. **Procedure:**

A. Security
1. The RCIC and MDC terminals will be maintained in a manner to ensure that no unauthorized person has access to the terminal or the RCIC, LEADS, and NCIC files contained within.
2. Non-certified persons shall not attempt the usage of the RCIC or MDC terminals.
3. All certified users will abide by all applicable laws and rules as established by RCIC, LEADS, and NCIC while operating the RCIC and MDC terminals, including but not limited to security, privacy, and confidentiality.
4. Terminals are for official use only. All violations will be investigated, and appropriate criminal or disciplinary actions will be taken.
5. RCIC terminals must be kept locked in a secure room with limited access.
6. No information from the RCIC or MDC terminals shall be given to any person not authorized to receive it. Persons authorized are limited to certified operators, and non-terminal agencies that have a participation agreement on file, signed by both parties, and submitted to LEADS.

7. All vendors having written contracts dealing with equipment or services in the terminal area must include LEADS security wording in the contract. Vendors must supply a list of personnel authorized for access to the area and equipment. Those listed must have completed the background check and security briefing requirements and this must be documented.
8. RCIC, LEADS, and NCIC will only be used for legitimate investigative purposes.

B. Computer Hardware
1. Only vendors authorized by RCIC may perform maintenance on RCIC equipment, except for routine cleaning of outside surfaces. No computer housing, chassis, monitor, keyboard, or accessory may be opened or otherwise accessed, except by authorized RCIC personnel.
2. No user may knowingly cause physical harm to any computer component belonging to RCIC.
3. No external devices, such as disk drives, scanners, cameras, etc., will be connected to the RCIC or MDC terminals.
4. The computer hardware and software are to be used only for the specific purpose of accessing the RCIC system or other law enforcement activities. RCIC prohibits the installation or use of games. This prohibition extends to any games or programs that are accessible via the internet or any other means.

C. Computer Software
1. No software may be added, modified, or removed from the system without the express written consent of RCIC. Antivirus software and updates will be provided and installed by RCIC personnel.
2. No removable media, such as CDs or flash drives may be used in the RCIC or MDC terminals.

D. Training
1. Every member of the UCPD who has access to RCIC information will be properly trained in the use of the RCIC computer system.
2. All operators are required to be LEADS/MDC certified within six months of hire.
3. All new employees will receive their security training and have it documented within 30 days of hire.
4. Recertification will be conducted bi-annually for all certified operators.
5. All certified operators are responsible for reading, signing, and dating the LEADing Newsletter when it is posted.

E. Terminal Uses
1. All uses of the terminals must be following LEADS rules defining official criminal justice purposes.
2. All operators must log in with their assigned username and password.
3. Terminals are not to be used for background checks for non-UCPD personnel.

4. Computer printouts are to be given to no one except authorized personnel. Operators must document who is given the printout if the person is not a UCPD employee. Criminal history and BMV printouts may only be removed from the Communications Center if documented and accounted for on the criminal history log. **NO ONE IS PERMITTED TO TAKE PHOTOS OF MDC SCREENS, RCIC TERMINAL SCREENS, OR RCIC PRINTOUTS FOR ANY REASON.**
5. Administrative messages/teletypes must be approved by the highest-ranking supervisor on duty and must notate who was responsible for the authorization.

F. Violations of RCIC, LEADS, and NCIC Policies
To meet the guidelines established by LEADS, the following actions will occur when violations of RCIC, LEADS, and NCIC policies have been determined to have occurred:
1. Any violations of LEADS policies must be reported immediately to the RCIC management staff.
2. A Computer Incident Report must be completed and faxed to RCIC as soon as possible to the attention of the RCIC manager or a member of the RCIC management staff no later than three days after the incident was discovered.
3. Any violations that have been determined to have occurred will follow the University of Cincinnati's discipline procedure. In extreme cases, criminal charges and termination may be imposed. RCIC has the right to prosecute for violations independent of the University of Cincinnati's disciplinary decision.

G. Warrant Entries
1. The Records Section is primarily responsible for warrant entries.
2. When the Records Section is unavailable, warrant entries shall be made by the ECC following UCPD policy 2.2.401 Warrant Completion Procedures.
3. The pick-up radius (PUR) for all warrants will be determined as follows:
   a. PUR 5 (Hamilton County only) – Non-violent felonies, simple assaults, crimes with no concern of harm
   b. PUR 4 (Hamilton County and adjacent counties) – any crime occurring at Clermont Campus
   c. PUR 3 (within 100 miles of Hamilton County within the state of Ohio) – Determined on a case-by-case basis. The shift supervisor must obtain approval from a captain.
   d. PUR 2 (the entire state of Ohio) – Determined on a case-by-case basis. The shift supervisor must obtain approval from a captain.
   e. PUR 1 (use extradition limits) – All robberies, burglaries, aggravated assaults, and any other crime where there is a concern for harm. The shift supervisor must obtain approval from a captain. All tier one offenses as defined in ORC 2935.01 shall be entered with a nationwide extradition radius. Extradition funding to reimburse local law enforcement agencies for the cost of in-state and out-of-state extraditions of dangerous wanted offenders back to Ohio to face criminal charges is now available through the Office of Criminal Justice Services (OCJS):

https://ocjs.ohio.gov/grants-funding-monitoring/grants-news/extradition-trans-port-reimbursement-funding-request-for-proposals-2022

4.   Warrant entries with PUR 1 through PUR 4 must include all available identifiers (vehicles, identification numbers, tattoos, etc.), including identifiers found on BCI and III printouts. If BCI or III contains a caution indicator, then the warrant entry should also contain a caution indicator. Printouts must be retained in the warrant file to back up the data entered. If BCI or III returns no match, the query result printouts must be retained in the warrant file to support the lack of data entered. The Records Section will run BCI/III and BMV queries and use the information to pack the record.

5. A warrant entry worksheet will be completed by the entering operator for each warrant entered. All entries will be checked by a second party and documented on the warrant entry worksheet. The second-party check can be performed by any ECD or records section staff. The completed worksheet will be kept in the warrant file in the Communications Center. TAC will conduct a final check to ensure LEADS and NCIC compliance.

6. Warrants will be removed by the Communications Center as soon as possible after the department is made aware of the arrest. Following the removal, a query should be performed to guarantee removal from all systems. Warrant removal will be documented on the warrant entry worksheet in the appropriate places by the ECD removing the warrant. After removal, the entire warrant folder will be forwarded to the records section.

H. Stolen Vehicles/Plates
1. Stolen vehicles/plates will be entered by the Communications Center.
2. Before entry, BMV must be queried to obtain owner and current registration information and compare the VIN number for accuracy. Printouts of BMV queries will be retained with the case file.
3. Entry will be documented on a vehicle entry worksheet by the entering ECD. All vehicle/plate entries will be checked by a second-party ECD and documented on the vehicle entry worksheet. Completed worksheets will be kept in the case file in the Communications Center.

I. Other Entries
The Records Section is responsible for entering all traffic history, criminal history, arrests, and stolen property. All entries will follow the format as outlined by the RCIC manual.

J. Hit Confirmations
UCPD will ensure that hit confirmations for warrants and stolen property are performed within the time frames established by RCIC, LEADS, and NCIC. The computer terminal will be monitored on a 24-hour basis in the Communications Center by Communications Center personnel. Hit confirmations will follow the procedures established by RCIC.

K. Validations
1. Warrants, stolen vehicles/plates, and stolen guns will be validated on a schedule

set by RCIC.

2. The issuing officer must contact the victim to verify prosecution is still desired. Next, the prosecutor must be contacted to verify the case is still prosecutable. Cases determined to be no longer prosecutable will be removed from RCIC by the Communications Center and dismissed via the court. When a warrant is removed, it will be documented on the warrant entry sheet by the ECD, and a query should be performed to ensure removal from all systems.

3. Warrants which are determined to be active will be updated by the TAC by performing the same queries used to pack the original entry and updating the warrant with any new identifiers. Printouts should be maintained in the warrant file to back up the data entered.

4. To validate stolen vehicles/plates, an investigator will contact the owner to verify the vehicle/plate has not been recovered. If the investigator is unable to validate a stolen vehicle or plate, a determination must be made by the assigned investigator along with the Investigations Supervisor on whether to remove the entry from the system. This will be determined on a case-by-case basis.

5. Stolen guns will remain entered if the offense report is on file, regardless of the ability to verify the status with the owner. Stolen gun entries will only be removed if the gun is recovered.

6. Once all listed records have been checked, the TAC will sign, date, and return the validation certificate to RCIC. Validation lists must be retained for one year.

7. All other stolen property not subject to validation will be reviewed annually by the TAC, and a determination made on whether to remove the entry from the system. This will be determined on a case-by-case basis.

References:

UCPD policy 2.2.401 Warrant Completion Procedures