



<b>SUBJECT:</b> <b>LEADS Access and Control</b>	PAGE <u>  1  </u> OF <u>  8  </u>
	<b>NUMBER: 05-OIT-02</b>
<b>RULE/CODE REFERENCE:</b> 4501:2-10-01 to 4501: 2-10-12; 4501: 2-10-14	<b>SUPERSEDES:</b> 05-OIT-02 dated 04/09/18
<b>RELATED ACA STANDARDS:</b>	<b>EFFECTIVE DATE:</b> <b>July 29, 2019</b>
	<b>APPROVED:</b> 

**I. AUTHORITY**

Ohio Revised Code 5120.01 authorizes the Director of the Department of Rehabilitation and Correction, as the executive head of the department, to direct the total operations and management of the department by establishing procedures as set forth in this policy.

**II. PURPOSE**

The purpose of this policy is to establish procedures for the use of, access to, and reporting of violations in reference to the Law Enforcement Automated Data System (LEADS).

**III. APPLICABILITY**

This policy applies to all persons employed by or under contract with the Ohio Department of Rehabilitation and Correction (ODRC). The procedures specifically apply to the ODRC LASO, all LEADS computer administrators, terminal agency coordinators, LEADS computer operators, and any other employee having access to the data received over LEADS.

**IV. DEFINITIONS**

**Data Privacy Point of Contact (DPPOC)** - The ODRC chief who is responsible for overseeing data privacy issues for the ODRC enterprise.

**DRC OnBase Administrator** - The ODRC Bureau of Sentence Computation and Records Management chief who is responsible for overseeing the operational management of the ODRC OnBase enterprise content management system.

**Criminal Justice Information Services (CJIS)** - Serves as the focal point and central repository for criminal justice information services in the FBI. This division provides identification and information services to local, state, federal and international criminal justice communities. The CJIS division includes the fingerprint identification program, national crime information center program, uniform crime reporting program, and the development of the integrated fingerprint identification system.

**Law Enforcement Automated Data System (LEADS)** - A statewide computerized information system and network established for criminal justice agencies within the State of Ohio. LEADS is administered by the Ohio State Highway Patrol (OSHP).

**LEADS Computer** - (This designation replaces the LEADS TERMINAL naming convention.) A computer workstation which has a static IP address and has had the LEADS software client installed. The connection to LEADS may be provided directly through the ODRC network or through the Virtual Private Network (VPN) but still has a static IP address.

**LEADS Computer Co-Users** - Ohio State Highway Patrol (OSHP), the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), the Bureau of Criminal Investigation and Identification (BCI&I) and various Intra-State systems, e.g., Northwest Ohio Regional Information System (NORIS).

**LEADS Computer Operator** - An ODRC employee or approved ODRC contractor who has successfully completed all LEADS training, testing, and certification requirements and is, therefore, defined as a “certified terminal operator” by LEADS.

**LEADS Coordinator** - The employee responsible for general oversight and supervision of LEADS within the ODRC. The LEADS coordinator in ODRC shall be the chief inspector or designee.

**LEADS Practitioner** - An ODRC employee who has successfully completed all required LEADS training and is authorized to receive LEADS data.

**LEADS Steering Committee** - A group responsible for preparing and publishing operating guidelines for users of the LEADS system. The committee is composed of representatives from the Ohio State Highway Patrol (OSHP), Buckeye State Sheriff’s Association, Ohio Association of Chiefs of Police, and the Bureau of Criminal Identification and Investigation.

**Local Agency Security Officer (LASO)** – The ODRC BITS chief who, in the capacity of the ODRC DPOCC, is responsible for overseeing LEADS information security for the ODRC enterprise which includes providing the appropriate secure computing hardware to ODRC LEADS users; serving as the primary LEADS information security liaison with the FBI, Ohio State Highway Patrol, Ohio Chief Inspector’s Office and other law enforcement or investigative agencies; distributing information security alerts and notifications to ODRC LEADS users; and maintaining LEADS information security documentation and assisting, when requested, with LEADS information security audits.

**Non-Terminal Agreement** - An agreement between LEADS and a criminal justice agency that does not have a LEADS computer that will permit the non-terminal agency access to information in the LEADS through any LEADS Access agency.

**OnBase** - An enterprise content management system utilized by ODRC for electronic document archival and retrieval. Access to OnBase is restricted to essential users only.

**Originating Agency Identifier (ORI)** - A nine-character identifier assigned by LEADS and NCIC to electronically address each agency and terminal within the agency.

**Records Destruction** - Destruction that occurs in such a manner as to render it unreadable. Preferred method of destruction is shredding.

**Terminal Agency Administrator (TAA)** - The ODRC deputy directors and/or their administrative designees responsible for the overall supervision of the LEADS computers and operators, appointment of Terminal Agency Coordinators (TACs), and the financial and physical security of the LEADS computers in their respective operational area.

**Terminal Agency Coordinator (TAC)** - The employee assigned the responsibility for supervision of the LEADS Computer(s) at their facility / office. This position is appointed by the TAA.

## V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (ODRC) to follow all rules and regulations that govern the use of the LEADS computer(s) and the data received through the use of this computer(s).

## VI. PROCEDURES

### A. Training for LEADS

1. The TACs shall be responsible for the training of LEADS operators, Level 2 practitioners and Level 4 information technology personnel by utilizing the CJIS Online Training. The TACs shall also be responsible for the disposal of the hard copy and below-noted logs, criminal justice offense records and manuals, when they are no longer needed.
2. The All Employee and Non-Escorted Contractor Security Awareness Training shall include at a minimum:
  - a. Individual responsibilities and expected behavior regarding being in the vicinity of CJI usage and/or terminals;
  - b. Implications of non-compliance;
  - c. Incident response (identify points of contact and individual actions);
  - d. Visitor control and physical access to spaces – discuss applicable physical security policy and procedures (e.g., challenge strangers, report unusual activity, etc.).
3. All employees and non-escorted contractors shall be provided with Security Awareness in the ELM System during:
  - a. New Employee Orientation;
  - b. Contractor Orientation;
  - c. Annual In-Service Training.
4. LEADS practitioners (Level 2) and IT personnel (Level 4) shall also be required to complete the CJIS Online Training within six (6) months of initial assignment and biennially thereafter.

5. The superintendent of the Corrections Training Academy (CTA) shall be responsible for providing a link to the CJIS Security Awareness Training through the ELM System and shall ensure all new and current employees complete the training during New Employee Orientation and Annual In-Service Training.
6. The agency LEADS administrator shall be responsible for the annual review of lesson plans or instructional materials utilized for the CJIS training to ensure compliance with LEADS policies.

#### **B. Location and Security of LEADS Computers**

1. LEADS computers shall be placed in a secure location with limited employee access. Only authorized persons shall be allowed in this area. The TAC shall provide a list of persons who have access to this location and this list shall be made available to the ODRC LASO and LEADS computer operators.
2. When left unattended, inquiry computers shall be secured in a manner so access cannot occur by unauthorized persons. The operator shall log off when leaving the computer area.
3. The LEADS computer must be available twenty-four (24) hours a day, seven (7) days a week for the authority to enter records (i.e., Warrant/Wants/Stolen Vehicles/etc.) into the LEADS/NCIC files. Supporting documentation (i.e., copy of want, case file, etc.) for all entries into LEADS/NCIC databases shall be maintained in a location that is readily available to the LEADS computer operator and shall be entered in a timely manner.

#### **C. Authorized Access to LEADS Computers and Related Information**

1. A TAC is to be assigned to monitor the use of each LEADS computer and ensure all rules and regulations are followed. LEADS, NCIC, NLETS, and BCI&I data files accessed through the LEADS computer(s) is data made available for restricted distribution and use by criminal justice agencies for criminal justice purposes. Misuse of the LEADS computer(s) and/or data could result in criminal charges, personnel action and/or the removal of the LEADS computer(s). Rules and regulations governing the use of the LEADS computer(s) must be followed in detail.
2. Access to data through the LEADS computer(s) is only for criminal justice agencies to be used for criminal justice purposes. A list of the Originating Agency Identifiers (ORIs) permitted access is in a database maintained by LEADS. The LEADS computer operator must use the ORI of the non-terminal agency. If not authorized to receive data, the inquiry must be rejected.
3. All Computerized Criminal History (CCH) record checks shall only be conducted for the use of criminal justice agencies. Non-terminal criminal justice agencies must have executed a Non-Terminal Agreement with LEADS. A current copy of this agreement shall be maintained at LEADS. A current copy of the non-terminal ORI shall be required upon request.

4. Aside from LEADS computer operators, only ODRC employees who are verified LEADS practitioners shall be authorized to receive LEADS data. LEADS practitioners shall adhere to all LEADS requirements pursuant to the information and instructions delivered by the TAC during mandatory LEADS training.
  - a. LEADS practitioners must request LEADS data from the appropriate TAC who may require a written request from the LEADS practitioner for purposes of documentation. If a written request is utilized, the request shall be maintained by the TAC pursuant to all LEADS requirements.
  - b. Prior to providing the requested data to the LEADS practitioner, the TAC shall verify the LEADS practitioner has successfully completed all required LEADS training and is, therefore, authorized to receive LEADS data.
  - c. Upon verifying the LEADS practitioner has successfully completed all required LEADS training and is, therefore, authorized to receive LEADS data and upon providing the requested data to the LEADS practitioner, the TAC shall document the transaction pursuant to all LEADS requirements.
  - d. If the TAC cannot verify the ODRC employee requesting the LEADS data successfully completed all required LEADS training and is, therefore, authorized to receive LEADS data, the TAC shall not provide the requested LEADS data to the ODRC employee until the LEADS practitioner successfully completes all required LEADS training is verified.
  - e. If the TAC suspects the ODRC employee requesting the LEADS data is misrepresenting their LEADS status in order to obtain LEADS data they are not authorized to receive, the TAC shall report the incident pursuant to section VI.C.8 of this policy.
5. Appropriate background investigations must be conducted on all LEADS computer operators and practitioners, including submission of a completed applicant fingerprint card to the FBI Identification Division through the state identification bureau. State and national arrest and fugitive files must be checked before system access is granted.
  - a. If arrest and fugitive records of any kind are found, access shall be delayed pending a review by the appropriate managing officer who shall, if necessary, consult with the ODRC chief inspector.
  - b. If the conviction is for a felony, the request shall be denied. Felony arrests without a conviction and non-felony arrests or convictions shall be reviewed by the managing officer who will determine if the request should be rejected or forwarded to the agency coordinator, who will then forward it to LEADS for consideration and a formal decision.

- c. Arrests or convictions of current authorized LEADS users shall also be reported to the agency coordinator, who shall forward it to LEADS for consideration and a final decision.
6. The TACs shall provide an official list of full-time employees who are authorized to request Computerized Criminal History (CCH) record check to the auditing staff of the OSHP and to the ODRC LASO. This list shall be reviewed bi-annually by the TAC to ensure it is still accurate. This list shall be provided to the LEADS coordinator and to the ODRC LASO.
7. The managing officer/designee shall advise the appropriate TAC when an employee's right to access has been terminated. Checks shall not be made unless the person making the request is on an authorized list.
8. All ODRC employees, regardless of their LEADS certification / use status, are required to immediately report any incidents which indicate a violation or possible violation of LEADS/NCIC/BCI&I/NLETS rules and regulations or ODRC policies and procedures to the ODRC LASO, LEADS TAC and LEADS coordinator pursuant to ODRC policy 01-COM-08, Incident Reporting and Notification. Verbal reports shall be immediately followed up with written notification, pursuant to ODRC policy 01-COM-08, Incident Reporting and Notification to the ODRC LASO, LEADS TAC and LEADS coordinator. The LEADS coordinator, in consultation with the ODRC LASO, shall make appropriate notification to the LEADS Steering Committee and the ODRC chief inspector. The chief inspector shall then determine the appropriate means of investigating the incident. Once an investigation is complete, a copy of the investigation shall be forwarded to the managing officer, regional director/designee, and the LEADS coordinator.

#### **D. LEADS Usage**

1. Validations of entries into LEADS/NCIC shall consist of, but not be limited to, the following: (1) Review of the case material to insure it is still active; and (2) A check with the Adult Parole Authority (APA) to ensure the warrant/want is in proper order. All inactive record entries shall be canceled immediately. Documentation of validation efforts must exist.
2. Response to inquiries concerning records entered through the LEADS computer must occur in a timely fashion as described in the LEADS/NCIC manuals. Hits confirmation formats (HCS.1/HCS.2/HCS.3) must be utilized.
3. No LEADS, NCIC or BCI&I data, reports, records, documents or printouts shall be scanned and uploaded into ODRC's OnBase content management system without the written approval of the ODRC OnBase administrator.

**E. Manuals and Documentation of LEADS Information**

1. LEADS, NCIC, and BCI&I manuals are available online to authorized personnel. If the manuals are copied by authorized personnel, they shall be placed in a location that is readily accessible to the TAC and all LEADS computer operators, be maintained in a chronological order, including the most current updates and/or additions provided by LEADS/NCIC/BCI&I., and be kept neat, orderly, and in good condition. When the manuals are no longer of any use, they shall be disposed of by authorized personnel in a secure manner via shredding or incineration in order to minimize the risk of sensitive information being accessed or compromised by unauthorized individuals.
2. An automatic log of all criminal history record checks is maintained and archived by the LEADS system. LEADS computer operators shall maintain a log of all criminal history record checks when a computerized criminal history record response is disseminated to an individual not employed by ODRC.
3. These log sheets are to be maintained in a file and placed by the month in which the inquiry was made. These logs shall be maintained for a period of one (1) year at which time they may be disposed of by authorized personnel in a secure manner via shredding or incineration in order to minimize the risk of sensitive information being accessed or compromised by unauthorized individuals.
4. These log sheets are to be maintained in a safe/secure location by the person making the request. All captions on the log sheets are to be completely filled out and must be typed or printed as follows:
  - a. Agency Name (Complete name of the agency with no abbreviations allowed);
  - b. ORI Number - A nine-digit number assigned to the LEADS computer;
  - c. Date the CCH inquiry is made;
  - d. Time the CCH inquiry is made in 24-hour time;
  - e. Place an "X" in the BCI&I/CCH column if the request is for an Ohio CCH record check;
  - f. Place an "X" in the FBI-III column if the request is for an FBI-III National Crime Information Center Record Check;
  - g. Name of the LEADS computer operator (first and last name). Operator name shall be recorded only when the inquiry is made;
  - h. Subject's name and BCI&I or FBI Number - Other identifiers include Social Security Number, Date of Birth, etc. and may be entered in this caption;
  - i. If Disseminated: Officer Name and requesting Agency - Enter the full name of the person and requesting agency to which the information is disseminated;
  - j. PUR CODE C-J – Enter "C" when the inquiry is for Criminal Justice purposes. Enter "J" when the inquiry is for employment within the Criminal Justice Agency or licensing. BCI&I, CCH & FBI III–indicate which transaction;
  - k. Receiving Officer Signature - If the paper record is taken with the person making the request, he/she must sign in this caption. If the paper record is mailed to another criminal justice agency, the name of the person and agency must be entered in this caption. All paper copies must be sent "Certified Mail - Return Receipt Requested." Once the receipt is received, it shall be stapled to the original log sheet. A signature is

not required if the paper record is not disseminated. Any exceptions to the above must be approved by the LEADS coordinator.

5. The rules and regulations of LEADS/NCIC/BCI&I/NLETS are to be reviewed by the TAC and all LEADS computer operators bi-annually to ensure compliance. As new rules and/or regulations are provided, the TAC, all LEADS computer operators and other appropriate employees are to read and initial the regulation. Documentation of this review shall be maintained by the TAC.
6. Though available in on online format, LEADS/NCIC newsletters are to be printed, read and initialed by the LEADS TAC computer supervisor and LEADS computer operators. The newsletters are to be filed in sequential number and/or date order to ensure each is readily available for reviewing.
7. All correspondence received or sent over the LEADS network shall be attached to existing manuals or directives or filed by month. The filed correspondence is to be maintained for a period of one (1) year at which time it may be disposed of by authorized personnel in a secure manner via shredding or incineration in order to minimize the risk of sensitive information being accessed or compromised by unauthorized individuals.

**Related Department Forms:**

Incident Report

DRC1000