CITY OF AKRON, OHIO
POLICE DIVISION
KENNETH R. BALL II, CHIEF OF POLICE

NUMBER	EFFECTIVE DATE	RESCINDS
P-2018-035	August 1, 2018	P-07-035 Issued 7-11-05
SUBJECT LEADS/NCIC Procedure		ISSUING AUTHORITY Chief Kenneth R. Ball II

I. POLICY

The Law Enforcement Automated Data System/National Crime Information Center system (LEADS/NCIC) is an integral and indispensable tool for law enforcement agencies to access necessary information on a variety of criminal justice matters. It is important that all employees have knowledge of the procedures associated with the use of the LEADS/NCIC operating system and adhere to all guidelines set forth in this procedure as well as by the LEADS/NCIC rules and regulations set forth in the Ohio Administrative Code Chapter 4501:2-10. Protection of the LEADS/NCIC information is vital: a.) to the needs of the law enforcement agency, b.) to be in compliance with public disclosure requirements, and c.) to properly abide by applicable record retention rules.

It is the purpose of this procedure to provide clear rules and procedures regarding the proper use of the LEADS/NCIC system. Improper use of the system or improper distribution of information obtained from the system could result in criminal, civil, and/or departmental sanctions.

This policy is in compliance and pursuant to Ohio Administrative Code Chapter 4501:2-10 Law Enforcement Automated Data System (LEADS).

II. DEFINITIONS

A. Criminal Justice Agency – As provided in LEADS Administrative Rules: courts, and a government agency, nongovernmental agency, or any sub-unit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part (more than fifty percent) of its annual budget to the administration of justice. Examples include prosecutor agencies, courts at all levels with criminal jurisdiction, corrections departments, probation departments, and parole departments.

B. Law Enforcement Agency – Includes all local, county, state, and federal police agencies that are responsible for the enforcement of criminal law.

C. LEADS (*Law Enforcement Automated Data System*) – The statewide computerized network which provides computerized data and communications for criminal justice agencies within the State of Ohio. LEADS is administered by the Ohio State Highway Patrol's Superintendent. LEADS serves as the electronic communication network for Ohio's criminal justice communities and the gateway to NCIC.

D. NCIC – *(National Crime Information Center)* – The nationwide computerized filing system established for criminal justice agencies at the local, state and federal levels, which is managed by the Federal Bureau of Investigations. It is a computerized index of open warrants, arrests, stolen property, missing persons, and dispositions regarding felonies and serious misdemeanors.

E. CCH *(Computerized Criminal History)* – An Ohio electronic data processing file which is accessible using specific data fields. It is a central repository for arrest, conviction, and disposition data on adults and juveniles arrested for felony and gross misdemeanor offenses. BCI is responsible for storing these records.

F. TAC *(Terminal Agency Coordinator)* – Each agency with LEADS/NCIC access shall appoint a TAC. A TAC is the designated person that serves as the point-of-contact at the local agency for matters relating to LEADS information access. A TAC administers LEADS systems programs within the local agency and oversees the agency's compliance with LEADS/NCIC system policies.

G. LEADS Inquiring Operator – Is any person certified to access either a LEADS mobile or workstation terminal. LEADS Inquiring Operators are certified through the Akron Police Department's TAC. Inquiring Operators do not have access to enter information into the LEADS/NCIC system. LEADS Inquiring Operators includes all certified Akron Police officers.

H. LEADS Terminal Operator – Is any person certified to access either a LEADS mobile or workstation terminal. LEADS Terminal Operators are certified through the Akron Police Department's TAC. Terminal Operators have access to enter information into the LEADS/NCIC system to include wanted persons, missing persons, stolen autos, etc.

I. LEADS Practitioner – Is any person authorized to receive LEADS/NCIC information who is not a certified Terminal Operator or a certified Inquiring Operator. LEADS Practitioners have access to LEADS/NCIC information however they cannot operate the LEADS terminal.

J. LASO *(Local Agency Security Officer)* - Each agency with LEADS/NCIC access shall also appoint a LASO. The LASO and TAC can be the same person. The LASO is the person designated as the primary information security contact between a local law enforcement agency and the CJIS System Agency (CSA). The LASO actively represents his/her agency in all matters pertaining to information security, disseminates information security alerts and other material to his/her constituents, maintains information security documentation (including system configuration data), assists with information security audits of hardware and procedures, and keeps the CSA informed of any information security needs and problems. The LASO will be responsible for overseeing the use of LEADS/NCIC hardware and software use and security.

K. LEADS Steering Committee – Is established to provide advice to the superintendent of the Ohio State Highway Patrol concerning the governing of LEADS.

III. PROCEDURE

A. GENERAL RULES AND GUIDELINES

1. Authorization and Access.

   a. Only authorized law enforcement personnel who have received the required training and are certified in the use in the LEADS/NCIC system will have access to utilization of the LEADS/NCIC system as designated by the Chief of Police.

   b. Access and retrieval of information from the LEADS/NCIC system must be related to the job duties of the authorized employee/user and the administration of criminal justice.

   c. Under no circumstances may the LEADS/NCIC system be utilized for any personal reason whatsoever and for any matter that is unrelated to the scope of the officer/operator's assigned job duties.

2. Confidentiality. All information retrieved from the LEADS/NCIC system is confidential. Information obtained from the LEADS/NCIC system shall only be used and shared with relevant parties in order to carry out the handling of a job related criminal justice matter. The information shall **NOT** be disseminated outside of the law enforcement or criminal justice agency/system or for purposes unrelated to the administration of criminal justice except pursuant to a information exchange agreement. Information, data, and statistics gathered or disseminated through the LEADS/NCIC system is exempt from Ohio's Public Records Law, except for as provided by law.

3. Consent. Use of the LEADS/NCIC system indicates consent to monitoring and recording of all information requested and obtained by the Employer.

4. Repair. Agency owned equipment used to access LEADS as the primary agency session shall be supported by a repair service as required by the LEADS security policy.

5. Postings/Notices.

   a. All LEADS/NCIC secure areas will have clearly posted signs indicating, ***"LEADS Access Area, Authorized Personnel Only".***

   b. Any system that accesses LEADS/NCIC information **SHALL** display an approved system use notification message that contains information that the user is accessing a restricted information system, and that the system usage may be monitored and subject to audit.

6. Impermissible use of information. LEADS/NCIC information ***may not*** be physically provided or delivered, posted, mailed, transferred, emailed, transported, or stored on phones or any other electronic devices or equipment or any form of media whatsoever outside of the Police Department.

7. Sanitization of Hardware. All hardware transferred externally must be sanitized using industry recognized standards and approved equipment and techniques. Hardware that is either transferred to a different department or to an employee without authorized access **MUST** be sanitized as hardware transferred externally.

8. Security and Protection of LEADS/NCIC Data. The responsibility for the security and protection of information obtained from the LEADS/NCIC computer system rests with all authorized employee(s) that obtain and use the information and the agency receiving such information. Authorized Akron Police Department personnel shall protect and control electronic and physical LEADS/NCIC information while at rest and in transit. The Akron Police Department will take appropriate safeguards for protecting LEADS/NCIC information to limit potential mishandling or loss while being stored, accessed, or transported.

    a. All devices with access to the LEADS/NCIC network must have adequate physical security to protect against unauthorized access.

    b. All visitors and vendors must be accompanied by authorized personnel at all times when accessing secure areas.

    c. LEADS/NCIC terminals must be physically positioned so unauthorized persons are unable to view the screen and must employ session lock mechanisms to prevent unauthorized access.

    d. To protect LEADS/NCIC information, Akron Police Department personnel **SHALL:**

        i. Securely store electronic and physical media within a physically secure or controlled location. A secured area includes a locked drawer, cabinet, or room.

        ii. Restrict access to electronic and physical media to authorized individuals only.

        iii. Ensure that only authorized users remove printed form or digital media from LEADS/NCIC.

        iv. Physically protect LEADS/NCIC information until the information is destroyed or sanitized using approved equipment and techniques.

        v. LEADS/NCIC information must not leave the employee's immediate control. LEADS/NCIC printouts cannot be left unsupervised while physical controls are not in place. Precautions must be taken to obscure LEADS/NCIC information from public view.

        vi. Remote access is not permitted to LEADS/NCIC except as provided by LEADS.

e. Any improper disclosure of LEADS/NCIC information, or information that is lost, stolen, or reported as not received, **MUST** immediately notify his or her supervisor **AND** the police department's LASO or TAC.

B. OFFICERS' RESPONSIBILITIES

1. Each operator is accountable for all transactions occurring while his/her assigned password is logged onto a terminal accessing LEADS. An audit trail shall be maintained for each dissemination, or receipt, or any printout of information from LEADS. Officers are required to log off the system at the end of their shift.

2. An officer shall only request that the LEADS operator initiate a hit confirmation from an outside agency warrant within the PUR (Pick Up Radius) when the officer has physical control of the person or property. The officer will be responsible for using confirmed information in establishing sufficient legal grounds for probable cause to arrest or seize property. Exceptions to this include hit confirmations on protection orders for officers issuing protection order violation warrants.

3. An officer requesting a Computerized Criminal History (CCH) shall provide the LEADS operator with an incident report number or a criminal case number regarding the subject inquired upon. Each LEADS CCH inquiry shall contain the applicable purpose code and be logged into the LEADS computer system by the LEADS operator.

4. In the event none of the above numbers have been obtained, a LEADS control number will be assigned. In such cases, the requesting officer **SHALL** submit a short confidential detailing the reason for the CCH and submit it to the LEADS Terminal Operator.

5. CCH information shall **NOT** be transmitted by radio or telephone except in emergency situations.

6. LEADS/NCIC and CCH printouts shall **NOT** be transferred to any personnel or agency outside the department as referenced under the Confidentiality section of this Policy.

7. When a printout is no longer needed for official purposes, the officer requesting and receiving the printout **WILL** destroy it to the point that it is no longer legible. Officers **WILL** make printouts unreadable prior to disposal.

8. The officer receiving the printout is responsible to make sure each page of the printout has been properly stamped by the LEADS Terminal Operator with the officer's name or personnel ID number as well as the date the printout was obtained. In addition, the officer will maintain security of the printout until the printout is destroyed.

9. Officers are required by LEADS/NCIC to be retested and recertified.

C. LEADS/NCIC TERMINAL OPERATORS' RESPONSIBILITIES

1. LEADS Terminal Operators are responsible for the security of LEADS/NCIC information when both disseminating and entering. Final responsibility for the security and confidentiality of criminal justice information retrieved through the computer equipment rests with the individual operator.

2. LEADS Terminal Operators are responsible for accessing and entering LEADS information through the LEADS/NCIC database and ensuring the information entered is accurate, complete, concise, timely, and verifiable.

3. LEADS Terminal Operators are responsible for maintaining an audit trail of all relevant information obtained or entered into the LEADS/NCIC system.

4. Operator **WILL** make printouts unreadable prior to disposal.

5. LEADS Terminal Operators are responsible for verifying all LEADS/NCIC printouts leaving the secured area have been properly stamped with the officer's name or personnel ID number as well as the date the printout was obtained.

6. Invalid records or data must be removed from the files immediately and may not be re-entered unless and until a complete validation of the data contained therein is completed.

D. ENFORCEMENT

1. All personnel who have access to LEADS/NCIC information have a responsibility to maintain the security of the information it contains and must ensure information is disseminated only to authorized personnel for the appropriate purpose. LEADS/NCIC information may only be shared for criminal justice purposes as related to the employee's job duties, as referenced under the Confidentiality section of this Policy.

2. Violations concerning the misuse of information could result in felony charges, departmental charges including loss of LEADS/NCIC terminal use by the member and the agency, or termination of employment.

3. Final responsibility for the security and confidentiality of criminal justice information retrieved through the computer equipment rests primarily with the individual operator.

4. Audits. All LEADS/NCIC, CAD, and MDB user accounts will be subject to a periodic and at least triennial audit conducted by members of the LEADS staff. The TAC is responsible for conducting audits. The TAC will also ensure that all users are valid, and will take appropriate steps to remove invalid users. The TAC will document the audit results and actions taken.

5. An audit trail **SHALL** be maintained by participating LEADS agencies by stamping each page across the body of the printout for each dissemination.

6. The Akron Police Department's TAC/LASO and supervisor in charge of the appropriate division included within the LEADS/NCIC information system **WILL** be advised of breaches of this policy and will be responsible for appropriate remedial action.

7. Violations of these rules may result in denial of access to LEADS. Violations of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action and may result in criminal prosecution, civil action, or departmental discipline up to and including termination from employment.

By Order Of

Kenneth R. Ball II
Chief of Police

Date 7-24-18