



North Carolina
Department of Information Technology
Criminal Justice Law Enforcement Automated Data Services
(CJLEADS)

**Policy for
Access to the CJLEADS Information System**

Revision Effective Date July 1, 2016

**North Carolina Department of Information Technology
4101 Mail Service Center
Raleigh, NC 27699-4101**

General Policy for Access to CJLEADS

1. The provisions set forth in this “General” section apply to all means of access to any information or application designated as a functionality or component of CJLEADS, under the management and operation of the Department of Information Technology (DIT) or any State agency assigned these responsibilities.
2. Data that is not classified as a public record under G.S. 132-1 shall not be considered a public record when incorporated into the CJLEADS database. S.L. 2010-31 s. 6.10(d) Redistribution of data not subject to public disclosure under the NC Public Records Act (N.C.G.S. Chapter 132) including, but not limited to, juvenile case data and unreturned criminal processes, is prohibited.
3. Each source agency providing data for CJLEADS shall be the sole custodian of the data for the purpose of any request for inspection or copies thereof under Chapter 132 of the General Statutes. Users of CJLEADS shall only allow access to data from the source agencies in accordance with rules adopted by the respective source agencies and shall maintain the confidentiality requirements attached to the information provided to CJLEADS by the various State and local agencies. S.L. 2010-31 s. 6.10(d)
4. Access to CJLEADS shall be granted to agencies only upon completion of a “License and Usage Agreement” between the Agency signatory authority and the State of North Carolina CIO or designee.
5. Inquiry access to criminal justice data shall be subject to the limitations set forth herein.
6. The DIT reserves the right, in its discretion, to limit or terminate access to CJLEADS due to security, performance issues and/or scheduled maintenance.
7. Agency or organization must provide facility and network information as well as user information to enable CJLEADS operations to set up and ensure adequate security and application integrity. Agency or organization must designate a technical contact to assist CJLEADS operation with managing and resolving any network or technical user access issues.
8. Agency or organization shall designate internal personnel as site administrators. Site administrators are agency users designated as such to DIT in the “Licensing and Usage Agreement”. A site administrator is responsible for:
 - a. Establishing the agency as an NCID organizational entity¹
 - b. Requesting NCID administrator rights for the NCID organization entity as well as termination of those rights if agency discontinues use of the CJLEADS application
 - c. Establishing and managing agency users of the CJLEADS application in NCID and CJLEADS user administration tool
 - d. Resetting passwords and unlocking accounts for agency users in NCID
 - e. Terminating users as required by the “Licensing and Usage Agreement”
 - f. Periodic review of CJLEADS user list
 - g. Maintaining current site administrator contact information with DIT Operations
9. Training in accordance with DIT requirements shall be required prior to access to the CJLEADS system. All time, travel and expenses incurred on behalf of the agency or organization for such training will be the responsibility of the agency.

¹NCID – The State of North Carolina’s standard identity management and access service provided to state, local, business and citizens users of North Carolina information systems.

10. Help Desk services will be provided by DIT Support Services. The agency or organization, however, must provide a primary and secondary point-of-contact within the agency to resolve user administration issues such as resetting password and unlocking accounts. Other access, system usage and data issues or questions will be referred to the Help Desk.
11. Electronic documentation for user administration policies and procedures as well as user guides for the CJLEADS application will be made available to agencies and organizations.

Information Protection Policy for CJLEADS

The provisions set forth in this "Information Security Policy" detail the security features of the CJLEADS information systems, and are therefore not subject to disclosure under the Public Records Act. N.C.G.S. 132-6.1(c).

1. User IDs

- a. Each individual accessing the CJLEADS application and information must be identified with a unique User ID. Only the individual with whom a User ID is uniquely associated will use the User ID. Shared or generic User IDs are prohibited. Shared or generic User IDs will be subject to termination of the users' and/or agency's access to CJLEADS.
- b. The secure NCID shall be used only on authorized state information systems, and shall not be used on other systems (such as a home PC, banking, or other computer systems) where unauthorized parties may obtain the User ID.
- c. NCIDs will be deactivated after 45 days of inactivity. The user will not be able to login to any systems using NCID and must request NCID reactivation by the agency NCID administrator.
- d. Inactivity of 90 days in the CJLEADS application will result in deactivation of CJLEADS access. The user will not be able to access the CJLEADS information system and must request that CJLEADS access is reactivated by the agency administrator.
- e. Upon employee termination, the user site administrator identified in the "Licensing and Usage Agreement" must immediately terminate CJLEADS access and notify DIT CJLEADS Operations within 8 hours of the employee's termination.
- f. CJLEADS information system will log all user activity. Logged activity will be available for audit purposes.

2. Passwords

- a. A password for access to the CJLEADS information systems shall not be revealed by anyone to anyone, including supervisors, family members, co-workers, or even CJLEADS Operations. CJLEADS Operations personnel will **never** contact a user and ask for their password. Any party claiming to be "from CJLEADS Operations" who asks for a user's password is an impostor.
- b. Users asked for their password shall not reveal their password under any circumstances, and the incident must be reported to the CJLEADS Operations as soon as possible.
- c. All passwords must follow, at a minimum, the NCID policy of having strong passwords. Strong password must have a minimum number of characters and utilize punctuation or special characters. For more information see the NC Office of Information Technology NCID policy. (See <http://www.scio.nc.gov/Mission/InformationSecurityManual.aspx> Reference Chapter 2, **Section 01 - Controlling Access to Information and Systems, Section id 020106 Managing Passwords**)
- d. Passwords shall not be written down, nor displayed in clear text on hard drives, diskettes, or other electronic media.
- e. Passwords used to access the CJLEADS information system shall be changed at least every 90 days.

4. Information Security

- a. Officials, officers, employees, contractors, and agents of a government agency or subdivision of such agency are granted access to the CJLEADS information system only for the performance of their official duties.
- b. Use of access to the CJLEADS information system for any purpose outside the scope of those duties shall result in disciplinary action up to and including termination as determined by the AGENCY, and civil and/or criminal liability. Failure to ensure appropriate access and use of the CJLEADS information system may result in the AGENCY's loss of access to CJLEADS.
- c. CJLEADS is an inquiry only application. Information in CJLEADS may only be printed using the application print utility which logs all print activity for audit purposes. Printed materials may only be disseminated to authorized personnel for the administration of criminal justice activities. Any information printed by users or the AGENCY from CJLEADS must be secured and must be properly destroyed when no longer required.
- d. Electronic storage of CJLEADS data on any media including hard drives, CD-ROMs, or other removable media, is not recommended; however, CJLEADS recognizes that the saving and sharing of specific criminal justice information may be necessary in the performance of criminal justice duties and responsibilities of the user. The management of and liabilities associated with securing and protecting criminal justice information or data saved to desktop or laptop computer or storage media is the responsibility of the user and user agency. Users shall at all times be subject to the FBI's CJIS Security Policy and Procedures for handling and storage of criminal justice information, including the proper access, use, and dissemination of Criminal History Record Information (CHRI) and Personally Identifiable Information (PII). Storage of CJLEADS data on a mobile communication device, smartphone or tablet, is prohibited.

Pursuant to NCGS §20-43 (a), DMV photographic images accessed via the CJLEADS information system are confidential and shall not be released except for law enforcement purposes.

5. Infrastructure and Asset Security

- a. The CJLEADS information system is a web based application.
- b. Updated anti-virus software must be installed on all desktop and laptop computers accessing the CJLEADS information system.
- c. Users must not leave a computer or laptop unattended when logged into CJLEADS, such that unauthorized personnel might use the computer and User ID to access the information contained in CJLEADS.
- d. All desktop and laptop computers with access to the CJLEADS information system, when not monitored directly, must have the following controls performed:
 1. user(s) logged out of the system;
 2. password-protected screen saver; or
 3. system shutdown, if other options are not available.
- e. All mobile communication devices (e.g. smart phones and tablets) with access to the CJLEADS information system, when not monitored directly, must have the following controls performed (Reference Appendix A):
 1. user(s) logged out of the system;
 2. mobile device to lockout after 10 minutes of non-use
 3. system shutdown, if other options are not available.

Signatory Authority for CJLEADS Access

1. The “License and Usage Agreement” for access to the CJLEADS information system must be signed by the signatory authority for the agency or organization requesting access before any access can be established.
2. A “License and Usage Agreement” signed by someone not authorized to bind the agency contractually will be rejected.
3. The signatory authorities for government entities are as follows:
 - a. N.C. State Agencies.
State agencies may have multiple employees or officers authorized to sign the “Licensing Agreement”. Agency personnel should consult with legal counsel for their agency in order to determine signatory authority.
 - b. N.C. County Governments.
 - 1) Chairperson of the Board of County Commissioners; or
County Manager, if designated by the Board of Commissioners; or
 - 2) The individual county agency’s hiring authority, if designated by the Board of Commissioners.
 - 3) Sheriff for deputies and employees of sheriff’s department
 - c. N.C. Municipal Governments.
 - 1) Mayor or equivalent; or
 - 2) City Manager, if designated by the City Council or its equivalent; or
 - 3) The individual municipal agency’s hiring authority, if designated by the City Council or its equivalent.
 - d. U.S. Government Agencies.
Federal government agencies may have multiple employees or officers authorized to sign the “Licensing Agreement”. Agency personnel should consult with legal counsel for their agency in order to determine signatory authority.
4. Verification of signatory authority must accompany the “Licensing and Usage Agreement”.
 - a. For state and federal agencies, agency legal counsel must provide written verification of an individual’s signatory authority before a “Licensing Agreement” will be accepted for that agency.
 - b. For county and municipal governments, verification may take any form certified by the custodian of the records for the governing body, such as a certified transcript of meeting minutes. Any delegation of signatory authority by a Board of Commissioners, or by a City Council or its equivalent, must be provided in writing.
 - c. No verification of signatory authority is required for a sheriff signing for deputies and employees of the sheriff’s department.


Access Policy for CJLEADS

1. Resale of any data accessed via CJLEADS information system is prohibited.
2. Printing or dissemination of any data accessed via CJLEADS information system, except for authorized use in the administration of criminal justice activities is prohibited.
3. The agency or organization is responsible for providing and maintaining client workstations, laptops as well as internet connectivity and/or wireless access such air cards.
4. The agency at its discretion may allow use of personal mobile communications devices (e.g. smartphones and tablets). The agency should ensure all personnel have read and understand the terms and conditions of use on a mobile device as written in Appendix A of this policy.
5. The agency or organization shall ensure that personnel have received required training in the authorized and appropriate use of the CJLEADS application.

Policy Adoption

This Policy for Access to the CJLEADS Information System was adopted and is effective July 1, 2016.


John Correllus, DSCIO


Date

Appendix A – Terms and Conditions for Mobile Version of the CJLEADS Application

Terms & Conditions

This CJLEADS mobile application is provided to authorized CJLEADS users who agree to the terms and conditions of its use as defined in the Policy for Access to the CJLEADS Information System.

User must change settings of the mobile device to lockout after 10 minutes of non-use.

User acknowledges the privacy and confidentiality risks inherent in wireless mobile technology and agrees to take precautions to protect CJLEADS content, user ids and passwords. CJLEADS data should not be viewed or disclosed to any individual not authorized to have access to the information. CJLEADS images or data should not be saved to a wireless device.

All terms and conditions of CJLEADS use apply when using this mobile application. All auditing policy and procedures apply to the use of CJLEADS via wireless mobile technology.

By using the CJLEADS mobile application, you agree to abide by the terms and conditions listed above.