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, 2021

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

The provisions set forth in this Policy for Access to the CJLEADS Information System apply to all means of access to any data or reports from CJLEADS, a criminal justice application under the management and operation of the North Carolina Department of Information Technology's Government Data Analytics Center (GDAC) or any successive State agency assigned oversight responsibilities.

I. General Policy for Access to CJLEADS

1. Access to CJLEADS shall be granted to law enforcement organizations or other criminal justice agencies ("Agencies," or singularly, "Agency") and its users only upon completion of a License and Usage Agreement between the Agency and GDAC ("CJLEADS Agreement"). Access to any data in CJLEADS shall be subject to the limitations set herein.

2. Data displayed or accessed in CJLEADS should be considered confidential and not a public record unless such information is classified as a public record under North Carolina law. Redisclosure of data not subject to public disclosure under the NC Public Records Act is prohibited. This confidential information includes but is not limited to the following:
    a. DMV data
    b. NC State Bureau of Intelligence data
    c. Federal criminal justice data
    d. Criminal case data from the Administrative Office of the Courts, including witness information
    e. Sex Offender data
    f. Personally Identifying Information
    g. Inmate data
    h. Juvenile case data
    i. Unreturned warrant data

3. Agencies shall only permit its direct employees and natural person contractors to receive credentials to access CJLEADS.

4. The Agency shall take full responsibility for maintaining, and ensuring any Agency user maintains, the privacy, security, and confidentiality of data in CJLEADS pursuant applicable federal and state laws and regulations.

5. The GDAC reserves the right, in its discretion, to limit or terminate access to CJLEADS due to security concerns, suspected or confirmed unauthorized use or redisclosure of data, system performance issues, or scheduled system maintenance.

6. The Agency must provide facility and network information as well as user information to enable GDAC Production Services to set up and ensure adequate security and application integrity. The Agency must designate a technical contact to assist GDAC Production Services with managing and resolving any network or technical user access issues.

7. The Agency shall designate internal personnel as site administrators. Site administrators are Agency users designated in writing to GDAC Production Services via the CJLEADS Agreement. A site administrator is responsible for:
    a. Establishing the Agency as an NCID organizational entity.[1]
    b. Requesting NCID administrator rights for the NCID organization entity as well as termination of those rights if the Agency discontinues use of the CJLEADS application.
    c. Establishing and managing Agency users of the CJLEADS application in NCID and CJLEADS User Administration Utility solely for authorized employees or natural person contractors of the Agency.
    d. Resetting passwords and unlocking accounts for Agency users in NCID.
    e. Terminating users as required by the CJLEADS Agreement.
    f. Periodically reviewing the CJLEADS user list.
    g. Maintaining current site administrator contact information with GDAC Production Services.

8. Sale of any data accessed via CJLEADS information system is strictly prohibited.

9. Printing or disclosure of any data accessed via CJLEADS information system, except for authorized use in the administration of criminal justice activities, is strictly prohibited.

10. The Agency is responsible for providing and maintaining devices, workstations, laptops, as well as internet connectivity or wireless access.

11. Each organization 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. Records generated by GDAC regarding CJLEADS are the custody of GDAC. All requests made to an Agency for records within or regarding CJLEADS shall be immediately forwarded to GDAC at CJLEADS@nc.gov. The Agency is not permitted to respond to such request with the data or records requested, but the Agency may advise the requester that they are not the custodians of those records and that request has been sent to GDAC.

12. Training is required to be completed prior to any users gaining access to the CJLEADS system. All time, travel and expenses incurred on behalf of the Agency for such training will be the responsibility of the Agency.

13. Help Desk services are provided by NC DIT and/or GDAC Production Services when assistance is needed with the activities listed in Section 7 above. The Agency 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.

[1] NCID – 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.

14. Electronic documentation for user administration policies and procedures as well as user guides for the CJLEADS application will be made available to Agencies.

II. Information Protection Policy for CJLEADS

1. The provisions set forth in this Information Protection Policy section detail the security features of the CJLEADS information systems. All security features, user credentials, and network information are confidential and not subject to disclosure under the Public Records Act. N.C.G.S. 132-6.1(c).

2. **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 strictly prohibited**. Shared or generic User IDs will be subject to termination of the users' or Agency's access to CJLEADS.
   b. Users' NCID username (also referred to as "NCID") and password shall only be used as a username for authorized state information systems, and shall not be used on other systems (such as a home PC, banking websites, social media sites, etc.) where unauthorized parties may obtain the User ID.
   c. NCIDs will be deactivated after 90 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 180 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 site administrator.
   e. Upon employee termination, the Agency site administrator identified in the CJLEADS Agreement must immediately terminate that user's CJLEADS access.
   f. GDAC Production Services will log all user activity. Logged activity will be available for audit purposes.

3. **Passwords**

   a. A password for access to the CJLEADS information systems shall not be revealed by any user to anyone, including supervisors, family members, co-workers, or even GDAC personnel. **GDAC personnel will never contact a user and ask for their password.**
   b. If asked, users should not reveal their password under any circumstances. If anyone claims to be from CJLEADS Operations or GDAC Production Services and asks for a user's credentials or password, the incident must be reported to the GDAC Production Services as soon as possible.
   c. All passwords must follow the NCID policy of having a strong password. Strong passwords must have at least 8 characters, and utilize uppercase and lowercase letters, numbers and symbols. For more information, please see the NC DIT NCID Frequently Asked Questions. (https://it.nc.gov/ncid- frequently-asked-questions)
   d. Passwords shall not be written down or 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 Privacy and 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 law enforcement and/or official government duties.**

b. **Users are subject to the FBI's Criminal Justice Information Services (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).**

c. 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 or criminal liability. Failure to ensure appropriate access and use of the CJLEADS information system may also result in the Agency's loss of access to CJLEADS.

d. CJLEADS is an inquiry- or query-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 Agency personnel for the administration of criminal justice activities.

e. Any information printed by users or the Agency from CJLEADS must be securely maintained and stored by users. Printed documents must also be properly destroyed when no longer needed in the user's performance of their official duties.

f. Any electronic information downloaded or captured by users, including in reports, screenshots, or other files, must be maintained securely and properly deleted when no longer needed in the user's performance of their official duties. The user and Agency must ensure the information is not recoverable, adhering to NIST Special Publication (SP) 800-88 Revision 1, Guideline for Media Sanitization found at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, or in compliance with another approved process or guideline utilized for destruction of confidential information.

g. 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 a mobile device, desktop or laptop computer, or storage media is the responsibility of the user and Agency. **Storage of CJLEADS data on a mobile communication device, smartphone or tablet, is prohibited.**

h. 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.

i. To protect data in CJLEADS, the Agency agrees to use and ensure all of its users comply with the following privacy safeguards to prevent an unauthorized use or disclosure of data in CJLEADS that is not classified as a public record under G.S. 132-1 or other applicable law ("Confidential Information"):

1) Maintain Confidential Information in the strictest confidence and carefully restrict access to this Confidential Information to any other individual, employee, entity, or third party on a need-to-know basis, as is reasonably required to accomplish the Agency's business purposes

and protect the Confidential Information from loss, misuse, unauthorized disclosure, or breach;

2) Implement corrective action to eliminate or negate any harmful effect that is known of an unauthorized use, access, acquisition, or disclosure of Confidential Information; and

3) To ensure Confidential Information privacy and security, implement and maintain a strong encryption algorithm that meets industry encryption standard criteria as defined by NIST Standards to encrypt all Confidential Information, while in transit.

j. In the event an Agency experiences a cybersecurity incident or significant cybersecurity incident as defined in G.S. § 143B-1320(a)(4a) and (16a), respectively, and any incident that is a violation of the North Carolina Identity Theft Protection Act, G.S. Chapter 75, Article 2A ("IT Security Incident") involving Confidential Information, Agency and its users shall comply with the following:

1) The Agency shall follow the State's incident reporting policy available here: https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Incident_Response.pdf.

2) The Agency shall notify GDAC as quickly as possible of an IT Security Incident in a time frame not to exceed twenty-four (24) hours, by contacting CJLEADS@nc.gov and 919-754-6950. At a minimum, such notification shall contain, to the extent known: the nature of the IT Security Incident, specific information about the sourcing agency's data compromised, the date the IT Security Incident occurred, the date Agency discovered or was notified, and the identity of any affected or potentially affected individual(s). The Agency shall update GDAC of the status of the IT Security Incident weekly until the IT Security Incident is mitigated and closed.

3) The Agency shall work collaboratively with GDAC, and if necessary, the organization that originally disclosed the affected data to CJLEADS to resolve the IT Security Incident, mitigate any damages, and notify any affected individuals. The Agency shall be responsible for any costs associated with inappropriate use or redisclosure of CJLEADS data by their Agency or users.

5. **Reports of Misuse by Users.**

a. If GDAC Production Services team receives a report of potential inappropriate or unauthorized usage of CJLEADS via the Reporting Misuse Web Form (CF-11) at it.nc.gov/programs/cjleads and/or by means of the CJLEADS Abuse and Fraud Hotline, the Team will:

1) Document the reported incident.

2) Research the alleged misuse and generate usage reports as needed for investigation of the complaint. No information will be provided to the individual reporting the complaint unless:

i. The reporting individual is the Agency Chief Executive, Primary Contact or CJLEADS Authorized Administrator for the individual who has allegedly misused the CJLEADS system;

ii. The reporting individual is requesting the information under court order or subpoena; or

iii. The reporting individual has consent from the user's Agency Chief Executive Officer.

3) Establish contact (via telephone and/or email) with the Agency Chief Executive, Primary Contact or CJLEADS Authorized Administrator and explain that a complaint/allegation of misuse was registered with the GDAC Production Services Team.

4) Provide the Agency Chief Executive, Primary Contact or CJLEADS Authorized Administrator written documentation of:
   i. Who filed the complaint or allegation and contact information (unless anonymous);
   ii. Username and User ID of the individual involved in the alleged misuse;
   iii. Circumstances of alleged misuse;
   iv. Detailed report of potential inappropriate activity; and
   v. Policy for Auditing the Access and Usage of CJLEADS.
5) Request a written explanation of the resolution of the issue.
6) Maintain complete copies of all reported complaints or allegation of CJLEADS unauthorized or inappropriate usage and the resulting investigation and resolution in accordance with NCDIT records retention policy. These documents shall be maintained in a confidential folder, accessible only by the GDAC Production Services audit team, manager and NCDIT Legal Services.

b. The Agency will:
1) Review the allegation and information provided by the GDAC Production Services Team.
2) Investigate the circumstances of the allegation and determine if the incident was or was not an instance of unauthorized use of CJLEADS.
3) Take appropriate disciplinary and/or criminal action if the investigation of the incident reveals unauthorized or inappropriate use of CJLEADS.
4) Provide GDAC Production Services written explanation of the resolution of the issue within 3 weeks of postdate delivery of CJLEADS complaint documentation. Retain all complaint, investigation, and resolution documentation on site, according to records retention policy for these materials set by the Agency.

6. **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. When not in use or monitored, Users must perform the following actions with all desktop and laptop computers with access to the CJLEADS information system:
1) Actively log out of the CJLEADS system;
2) Utilize a password-protected screen saver that automatically turns on after no more than 15 minutes of inactivity; or
3) Shutdown the desktop or laptop computer device if other options are not available.
e. When not in use or monitored, Users must perform the following actions with all mobile communication devices (e.g. smart phones and tablets) with access to the CJLEADS information system:
1) Actively log out of the CJLEADS system;
2) Set mobile device to lockout after 10 minutes of inactivity; or
3) Shutdown the mobile device if other options are not available.

7. **Termination of Access and Destruction of Data**
   a. Upon the revocation of access to CJLEADS or in the event the Agency requests to terminate its access to specific sourcing Agency data, the Agency and its users shall comply with Sections 4(c) and (d) of this Part II regarding the destruction of any Confidential Information provided by the sourcing agency. The Agency shall also certify in writing within thirty (30) calendar days of such destruction of Confidential Information that all Confidential Information received by Agency or its users has been destroyed as required; and
   b. Until the Agency has certified completion of destruction of the Confidential Information in accordance with the destruction requirements outlined above in Section 3(c), the Agency and its users shall continue to comply with the terms of the CJLEADS Agreement and this policy.
   c. Upon Agency termination, GDAC will immediately terminate CJLEADS access.

III. Policy for Auditing the Access and Usage of CJLEADS

1. **Statement of Purpose:**
   a. The Agency is responsible for ensuring their Agency CJLEADS users are authorized, and their use and distribution of information is conducted solely for official law enforcement or criminal justice functions.
   b. The Policy for Auditing the Access and Usage of CJLEADS details the Agency's and GDAC's responsibilities to ensure that personnel are authorized for access to the CJLEADS application.

2. **General Policy for Annual CJLEADS Usage Audits**

   a. The provisions set forth in this "General" section apply to all means of auditing access to any information or application designated as a functionality or component of CJLEADS, under the management and operation of GDAC or any State Agency assigned these responsibilities.
   b. GDAC Production Services will:
      1) On an annual basis, create and distribute the Agency audit package via secure email or post to the Agency's Chief Executive Officer, Primary Contact or CJLEADS Authorized Administrator. The audit package shall contain:
         a. Audit Letter of introduction and instructions for completing the Agency audit;
         b. Standard reports as listed in item 2; and
         c. Audit Verification Form (CF-5) to be returned upon the completion of the Agency review of audit information.
      2) Provide standard reports in the Agency audit package to include but not limited to:
         a. Agency Usage Identical Record Report – compares records accessed and shows any users who display a pattern of continuously accessing the same record over a period of time.
         b. Agency Usage Exception Reports - various reports that display when a user falls outside the normal usage and patterns for the Agency. Upon the agencies request, GDAC Production Services will follow up on any unusual activity as needed.
      3) Confirm receipt of the audit package with the Chief Executive Officer, Primary Contact or CJLEADS Authorized Administrator, as designated in the signed CJLEADS Agreement.

4) Answer any questions or provide additional information as needed to complete the audit for the Agency.
5) Maintain completed copies of all Agency Audit packages and Agency responses in accordance with NCDIT records retention policy.

c. Agency will:
1) Review the Audit Package and instructions for completing the audit.
2) Verify all active Agency CJLEADS users, which requires Agency to:
    a. Review Agency Authorized User List and confirm that all users are current Agency personnel who are still authorized for access to CJLEADS application;
    b. Take appropriate action for any users on the Agency Authorized User List whose access requires adjustment, i.e., access termination or change of role; and
    c. Confirm on the Audit Verification Form (CF-5) that all users have been reviewed and appropriate action has been taken for required user authorization changes.
3) Review Agency Usage Exception and Identical Record Reports to investigate any usage falling outside the standard usage and patterns for the Agency.
    a. Review individual users' access and usage patterns as highlighted on exception reports.
    b. Review the user's summary level activity and determine if additional detailed reports are needed to conduct further investigation.
    c. Request and review detailed activity reports from the GDAC Production Services Team as needed to verify authorized/unauthorized use of CJLEADS.
    d. Confirm (via email or post) that appropriate action has taken place for any active Agency user whose usage was deemed by the authorizing organization to fall outside standard and authorized criminal justice purposes.
    e. Retain documentation on site for all investigations, according to records retention policy for audit materials.
4) After the completion of the annual review, the Chief Executive Officer, Primary Contact or CJLEADS Authorized Administrator for each Agency will sign the Audit Verification Form (CF-5). This form shall be returned to GDAC Production Services team within 3 weeks of postdate delivery of the CJLEADS Audit letter Form (CF-6). The Chief Executive Officer, Primary Contact or CJLEADS Authorized Administrator of the Agency must submit a signed copy of the form and email it to GDAC Production Services. Wet or verified digital signatures (e.g., DocuSign) are acceptable. Documents with wet signatures should be scanned and converted to a PDF or similar document format. If an Agency does not have scanning capabilities, the signed form will be accepted via fax 919-754-6947 or mail.
5) Retain all audit review documentation on site according to records retention policy for audit materials set by the Agency.

IV. Policy for Requesting User Audit Information and Offender Information

1. Requests for Agency Audit Information.

a. An Agency Chief Executive, Primary Contact or CJLEADS Authorized Administrator may request detailed audit reports regarding an Agency user's access to or usage of CJLEADS data. To request detailed audit information about Agency users, complete Report Request Form(s) CF7 – CFl0 found on it.nc.gov/programs/cjleads and submit to the GDAC Production Services Team.
b. CJLEADS audit reports detailing access to or usage of CJLEADS data is limited to the Agency's authorized users. Should an Agency need information about usage or activities of another Agency's authorized user, the Agency seeking the information must obtain a search warrant, subpoena, or other court order to obtain this information. Alternatively, the Agency can also request permission from the other Agency's Chief Executive Officer or CJLEADS Authorized Administrator to obtain the detailed audit report. The other Agency's Chief Executive Officer or CJLEADS Authorized Administrator can either (i) send a written request to the GDAC Production Services Team permitting the Team to disclose the report to the Agency, or (ii) provide the Agency with a detailed audit report the other Agency has in its possession.
c. **Notwithstanding the foregoing, the NC State Bureau of Investigation is entitled to review and receive detailed audit reports of CJLEADS user activity regarding all North Carolina Agencies without obtaining a search warrant, a court order, or subpoena.**

2. **Requests for Offender Reports.**

a. The GDAC Production Services Team cannot release offender records unless the requestor has sought a subpoena, warrant, or court order for such information and the source organization that has provided the requested data to CJLEADS has permitted its disclosure. This could require notifying multiple State and local agencies, and these agencies may contest the legal process.
b. In addition, GDAC is prohibited from disclosing federal criminal history record information to third parties. Persons seeking this information should contact the NC State Bureau of Investigation and review 14B NCAC 18B Section .0400 for instances when this information is permitted to be viewed or disclosed.

V. Signatory Authority for CJLEADS Agreement

1. The CJLEADS Agreement for access to the CJLEADS information system must be signed by the signatory authority for the Agency requesting access before any access can be established.

2. A CJLEADS 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 CJLEADS 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;
   2) The individual county agency's hiring authority, if designated by the Board of Commissioners; or
   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;
   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 CJLEADS 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 CJLEADS Agreement.
   a. For state and federal agencies, agency legal counsel must provide written verification of an individual's signatory authority before a CJLEADS 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.

This Policy for Access to the CJLEADS Information System is effective July 1, 2021.

DocuSigned by:
John Correllus
25E7727DB7B346B...

John Correllus
Deputy State Chief Information Officer
GDAC Director
NC Department of Information Technology

5/24/2021 | 9:01 AM EDT
Date

Summary of Policy Changes

Location or Section	Summary of Changes Made	Effective Date
Throughout the Policy document	Reordered certain subsections	7/1/2021
Introduction	Moved original Section I(1) to the introduction	7/1/2021
Section I	Clarified confidential nature of the CJLEADS data and included new examples; Clarified the responsibility of Agencies and users regarding the confidentiality of data	7/1/2021
Section II (2): User IDs	Removed requirement for notification of a user's employment termination	7/1/2021
Section II (4): Information Privacy and Security	Added requirement to securely stored and properly deleted utilizing NIST Special Public 800-88 revision 1 or other similar standards; Added new privacy safeguards; added requirements regarding cybersecurity incidents including notification of GDAC by Agency and responsibility of Agency for such incidents caused by Agency	7/1/2021
Section II (5): Reports of Misuse by Users	New subsection originally included in the CJLEADS Audit Policy regarding Agency reports of system or data misuse by users	7/1/2021
Section II (7)	New subsection regarding termination of Agency access to CJLEADS and destruction of data	7/1/2021
Section III	New section originally included in CJLEADS Audit Policy regarding auditing Agencies use of CJLEADS	7/1/2021
Section IV	New section regarding requests for user activity information and for offender information stored in CJLEADS; Authorized NC State Bureau of Investigation to access user activity audit reports of any North Carolina Agency without the need for a warrant, subpoena, or other legal process	7/1/2021