This USER AGREEMENT made and entered into by and between the North Carolina State Bureau of Investigation (SBI), Criminal Information and Identification Section (CIIS), and the above approved non-criminal justice agency (hereinafter "User Agency") as defined and set forth in the North Carolina Administrative Code (NCAC), for the purpose and consideration hereafter set out.

I. PURPOSE

A. The purpose of this User Agreement is to outline the requirements that must be followed in operating a device connected, either directly to or through another computer, to the Division of Criminal Information Network (DCIN). DCIN serves as the North Carolina's Criminal Justice Information Services (CJIS) computer system, responsible for the exchange of state and national criminal justice information to and from the following computer networks:

1. NCIC (National Crime Information Center);
2. Nlets (International Justice and Public Safety Network);
3. DMV (NC Division of Motor Vehicles);
4. AOC (North Carolina Administrative Office of the Courts);
5. DPS (North Carolina Department of Public Safety); and
6. NICS (National Instant Criminal Background Check System)

B. User Agency is responsible for the implementation and adherence to this User Agreement.

II. DEFINITIONS

As used in this User Agreement, the following terms shall have the meanings established below:

1. "Administration of criminal justice" means detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudications, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, "administration of criminal justice "includes crime prevention programs to the extent access of criminal history record information is limited to law enforcement agencies for law enforcement programs and the result of such checks will not be disseminated outside the law enforcement agency.
2. "Advanced Authentication" means an alternative method of verifying the identity of a computer system user. Examples include software tokens, hardware tokens, and biometric systems. These alternative methods are used in conjunction with more traditional methods of verifying identity such as user names and passwords.
3. "CJIS Security Addendum" means an uniform addendum to an agreement between a User Agency and a private contractor, approved by the United States Attorney General, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains other provisions as the Attorney General may require.
4. "CJIS Security Policy" means a document published by the CJIS Information Security Officer that provides criminal justice and non-criminal justice agencies with a minimum set of security requirements for the access to CJIS systems to protect and safeguard criminal justice information, whether in-transit or at rest.

5. "Criminal Justice Information" or "CJI" means the data provided by the Federal Bureau of Investigation to law enforcement to perform their mission and enforce laws, including, but not limited to: biometric information, identity history, person, organization, property, case or incident history data, and data provided by the Federal Bureau of Investigation necessary for civil agencies to perform their mission.
6. "Criminal Justice Information Services" or "CJIS" means Criminal Justice Information Services, which is a division of the Federal Bureau of Investigation. This division is responsible for the collection, warehousing, and timely dissemination of relevant criminal justice information to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.
7. "DCIN Device" means an electronic instrument used by a certified DCIN user to accomplish message switching, inquires, functional messages, and other DCIN, NCIC, or Nlets file transactions within DCIN.
8. "DMV Information" means information maintained by the North Carolina Department of Motor Vehicles to include vehicle description and registration information, and information maintained on individuals to include name, address, date of birth, license/customer identification number, license issuance and expiration, control number issuance, and moving vehicle violations and/or convictions. This list is not all-inclusive.
9. "National Crime Information Center" or "NCIC" means an information system maintained by the Federal Bureau of Investigation that stores criminal justice information which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.
10. "NCIC Operation Manual" means the document produced by CJIS that instructs individuals on the proper usage of NCIC. This document also contains requirements for systems that interface with NCIC. This document is posted within the DCIN end user interface.

III. ESTABLISHMENT OF A POINT OF CONTACT

A. User Agency agrees to designate an individual, under its direct management and control, as a Point of Contact (POC). The POC will serve as the point of contact at the User Agency for matters relating to DCIN access and training. The POC will administer DCIN system programs within the User Agency and oversee the User Agency's compliance with DCIN and CJIS system policies.

B. The POC may designate one or more assistant POCs (APOC) to assist in the duties of the POC role.

IV. MANAGEMENT CONTROL REQUIREMENTS

A. Personnel with access to criminal justice information obtained through DCIN and personnel who have a direct responsibility to configure or maintain computer systems or networks transmitting or storing criminal justice information obtained through DCIN must be under the management and control of the User Agency.

B. The degree of management control shall be such that the individual in charge of the User Agency has the authority and duty set forth in 12 NCAC 4F .0201 and .0202. In addition, the degree of management and control shall be such that the individual in charge of the User Agency has the authority to set standards for selection, supervision, and separation of personnel who will have access to criminal justice information as defined within the current FBI Criminal Justice Information Services (CJIS) Security Policy.

C. In instances where the User Agency utilizes a private contractor for the direct responsibility to configure or maintain computer systems or networks that transmit or store criminal justice information, the User Agency and private contractor shall enter in to a Private Contractor User Agreement in accordance with the current CJIS Security Policy, and shall incorporate the CJIS Security Addendum into said agreement.

V. DATA COLLECTED AND STORED

User Agency will not contribute to or store any information in any DCIN or CJIS system.

VI. PHYSICAL AND PERSONNEL SECURITY

The sensitivity and confidentiality of the information which is maintained in or provided by DCIN requires that each of the following measures be taken by the User Agency:

1. Any device used to access criminal justice information shall be located within a physically secure location as defined within the current CJIS Security Policy, and accessible only authorized personnel. Devices not located within a physically secure location shall used Advanced Authentication measures, as described in the current CJIS Security Policy, to safeguard against unauthorized access to any criminal justice information stored electronically by the User Agency.
2. Only those individuals who have received security awareness training shall be permitted to access or use any device to access any criminal justice information stored electronically by the User Agency.
3. Individuals with a direct responsibility to configure or maintain computer systems or networks that transmit or store criminal justice information shall be subject to the same background investigation and restrictions as those for potential DCIN users.

VII. TRAINING

A. Security awareness training shall be required within six months of initial assignment and every two (2) years thereafter for any individual under the management and control of the User Agency who has access to DCIN devices, has access to any network or computer system that stores, processes, or transmits CJI, or has either physical or logical (electronic) access to CJI.

   1. Security awareness training shall be provided by CIIS.
   2. User Agency shall keep records of all individuals under its management and control, including information technology personnel who service the User Agency, who have completed security awareness training. This documentation shall be made available to CIIS for auditing purposes.

VIII. INFORMATION USE AND ACCESS

User Agency agrees access to or dissemination of criminal justice information, including but not limited to criminal history record information (CHRI), obtained by the User Agency from or through DCIN, NCIC, or Nlets is restricted to purposes set forth in Section 151 of the Adam Walsh Child Protection and Safety Act of 2006.

IX. DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

Each User Agency obtaining CHRI through DCIN, NCIC, or Nlets shall comply with the following:

1. The User Agency shall maintain a dissemination log on all CHRI sent or received through DCIN for a period of not less than one (1) year.
2. The User Agency shall restrict the written, electronic, or oral dissemination of CHRI received through DCIN to authorized criminal justice and authorized non-criminal justice agencies with the exception of persons or agencies approved under 12 NCAC 04F .0405 and 12 NCAC 04E .0203.

X. HIT CONFIRMATION

User will not be responsible for any hit confirmation procedures.

XI. VALIDATIONS

User agency will not be responsible for the validation of any data entered in to any DCIN or CJIS sytem.

XII. AUDITS

A. In accordance with 12 NCAC 04F .0801, CIIS will conduct a biennial audit of the User Agency. This audit will examine all criminal justice information entered, modified, cancelled, cleared, and disseminated by the User Agency. The audit shall include, but is not limited, to, the following items:

1. criminal history record information usage; and
2. security safeguards and procedures adopted for the filing, dissemination, storage, and destruction of criminal justice information

B. In accordance with the CJIS Security Policy, the North Carolina Department of Justice Information and Technology Division (ITD) will conduct a biennial security audit of the User Agency. This audit will assess the User Agency's adherence to the CJIS Security Policy with regards to security of computer systems, networks, and devices with access to criminal justice information, and personnel security measures for those individuals with access to computer systems networks, and devices with access to criminal justice information.

XIII. ADMINISTRATIVE RULES

A. Use of and access to information contained within DCIN is subject to Title 12, Chapter 4 of the North Carolina Administrative Code (NCAC), which is incorporated herein to this User Agreement by reference.

B. Any future amendments or revisions to the NCAC will be provided to the User Agency and will be considered a part of this agreement and incorporated herein by reference.

XIV. TECHNICAL SECURITY

In the event User Agency utilizes a computer system or network to store or transmit criminal justice information it shall implement or ensure implementation of the following technical security controls in order to safeguard criminal justice information received from DCIN:

1. Designate an individual within the User Agency as the Local Agency Security Officer (LASO). The LASO shall have the following duties:
    a. serve as a point-of-contact for the North Carolina Department of Justice Information Security Officer (ISO);
    b. identify who within the User Agency uses devices that access criminal justice information and ensure no unauthorized individuals, computer systems, or networks have access to these devices or their respective networks;
    c. ensure that personnel security screening measures are being followed in accordance with the current CJIS Security Policy;

   d. ensure that CJIS and SBI-approved security measures are in place and working properly; and
   e. support policy compliance and ensure the ISO is promptly informed of security incidents.
2. Protect the boundary of its networks and information system(s) by:
   a. controlling access to networks processing criminal justice information;
   b. monitoring and controlling communications at the external boundary of the information system and at key internal boundaries within the system;
   c. ensuring any connections to the Internet, other external networks, or information systems occur through controlled interface (e.g. proxies, gateways, routers, firewalls, encrypted tunnels);
   d. employing tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use;
   e. ensuring the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall fail “close”); and
   f. allocating publicly accessible information system components (e.g. Web Servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual hot shall follow guidelines for virtualization set forth in the current version of the CJIS Security Policy.
3. Ensure proper encryption standards are met by:
   a. ensuring encryption is, at a minimum, 128-bit;
   b. ensuring criminal justice information is protected via cryptographic mechanisms (encryption) when transmitted outside the boundary of a physically secure location under the User Agency’s management and control;
   c. when criminal justice information is stored electronically outside the boundary of a physically secure location under the User Agency’s management and control, ensuring that it is protected via cryptographic mechanisms (encryption);
   d. ensuring that when encryption is employed, the cryptographic module used is certified to meet Federal Information Processing Standards (FIPS) 140-2 standards;
   e. if the User Agency uses a public key infrastructure (PKI) technology, developing and implementing a certificate policy and certification practice statement for the issuance of PKI certificates used in the information system. Registration to receive a PKI certificate shall:
      i. include authorization by a supervisor or responsible official;
      ii. be accomplished by a secure process that verifies the identity of the certificate holder; and
      iii. ensure the certificate is issued to the intended party.
4. Implement network-based and/or host-based intrusion detection tools.
5. Identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. The User Agency (or the software developer/vendor in cases where the software developed is maintained by a vendor/contractor) shall develop and implement a local policy that ensure prompt installation of newly released security relevant patches, service packs, and hot fixes. Local policies shall include the following items:
   a. testing of appropriate patches prior to installation;
   b. rollback capabilities when installing patches, updates, etc.;
   c. automatic patch updates without user intervention;
   d. centralized patch management; and
   e. the immediate addressing of patch requirements discovered during security assessments, continuous monitoring, or incident response activities.

6. Implement malicious code protection that includes automatic updates for all systems with Internet access. The User Agency shall implement local procedures to ensure malicious code protection is kept up to date on systems not connected to the Internet.
7. Employ virus protection mechanisms to detect and eradicate malicious code (e.g. viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers, and devices on the network. Malicious code protection shall be enabled on all of the aforementioned critical points and information systems and resident scanning shall be employed.
8. Employ spam and spyware protection.
    a. Spam and spyware mechanisms shall be employed at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
    b. Employ spam and spyware protection at workstations, servers, and/or devices on the network.
    c. Spam and spyware protection mechanisms shall be used to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes, compact discs, thumb/USB drives) or other removable media as defined within the current version of the CJIS Security Policy.
9. Employ a personal firewall on all mobile devices accessing criminal justice information. For the purposes of this User Agreement, a personal firewall is an application that controls network traffic to and from a device, permitting or denying communications based on policy. At a minimum, the personal firewall shall:
    a. manage program access to the Internet;
    b. block unsolicited requests to connect to the device;
    c. filter incoming traffic by IP address or protocol;
    d. filter incoming traffic by destination ports; and
    e. maintain an IP traffic log.
10. Prevent criminal justice information from being transmitted unencrypted across the User Agency's public network.
11. Block outside traffic that claims to be within the User Agency.
12. Any web requests to the User Agency's public network that are not from the internal web proxy shall not be passed.

XV. PENALTIES

A. The SBI reserves the right to immediately suspend access to criminal justice information when the North Carolina CJIS System Officer (CSO) determines that any of the above provisions of this User Agreement, any federal or state laws, or any provisions of the current version of the CJIS Security Policy have been violated.

B. Penalties for any violation of this User Agreement could involve federal or State sanctions or prosecution under existing laws relating to unauthorized access of computer data.

C. The SBI may reinstate access upon receipt of satisfactory assurances that any violation(s) did not occur or have been corrected and will not likely reoccur.

XVI. AMENDMENTS AND TERMINATION

A. The SBI reserves the right to amend this User Agreement as required by the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Nlets or based on other sound business practices. Any amendments to this Agreement shall be in writing and agreed upon by the parties.

B. The SBI reserves the right to terminate this User Agreement upon determination by the CSO of any of the following:

1. any applicable law, rule, or regulation has been violated;
2. the terms of this User Agreement have been violated; or
3. the User Agency no longer desires DCIN access.

C. Either party has the right to terminate this User Agreement after a thirty-day (30) written notice is provided to the other party named in Section XVII of this Agreement.

XVII. CERTIFICATION

I certify that I am the duly authorized representative of the North Carolina State Bureau of Investigation (SBI), Criminal Information and Identification Section and I will uphold this agreement.

By: _____ Date: _____
Wendy L. Brinkley
Special Agent in Charge
North Carolina CJIS System Officer (CSO)

I certify that I have read and understand the requirements for this agreement, and I will uphold this agreement. I further certify that I am the duly authorized head of below User Agency.

By: _____
PRINT TITLE / NAME AGENCY HEAD

_____
SIGNATURE AGENCY HEAD

_____
DATE

_____
PRINT AGENCY NAME

In the event that the management control is jointly shared by more than one criminal justice agency, the agency head of each agency with management control shall also affix their seals and signatures and shall uphold the provisions contained therein.