NEW JERSEY CRIMINAL JUSTICE INFORMATION SYSTEM

USER AGREEMENT

BETWEEN

THE NEW JERSEY DEPARTMENT OF LAW AND PUBLIC SAFETY,
DIVISION OF STATE POLICE,

OFFICE OF INFORMATION TECHNOLOGY

AND

JERSEY CITY POLICE DEPARTMENT  ORI # NJ0090600

(CRIMINAL JUSTICE AGENCY)

hereinafter "User," (a criminal justice agency as defined by New Jersey Administrative Code 13:59-1.1 and federal regulations, Title 28 - Judicial Administration, Chapter 1 - Department of Justice, Part 20 - Criminal Justice Information Systems (CJIS), Section 20.3(c) - "criminal justice agency," and further delineated in Section 20.3(d) - "administration of criminal justice") hereby agree to exchange such criminal history record information (CHRI), data pertaining to wanted/missing/unidentified persons, stolen property information, motor vehicle registration/driver license records, and other police information to the extent that such data is exchangeable in accordance with the laws of New Jersey and the United States and consistent with the conditions under which the information is disseminated for the administration of criminal justice and enforcement including the State's motor vehicle and traffic laws, and as is available via the New Jersey Criminal Justice Information System (NJCJIS), in the files of the National Crime Information Center (NCIC) and the New Jersey Wanted Person System (NJWPS), or obtained via the New Jersey and National Law Enforcement Telecommunications Systems (NJLETS and NLETS), and via NJCJIS access of the files operated and maintained by the New Jersey Motor Vehicle Commission (NJMVC).
**Introduction.** The New Jersey State Police, as part of the CJIS management, serves as the NCIC and NLETS CJIS Systems Agency (CSA) for the State of New Jersey. The NJCJIS is operating under the concept that management and responsibility should be shared. The various entities involved in operating, administering, controlling, and supporting the system; the FBI, the New Jersey State Police, the Office of Information Technology (O.I.T.), system users at the federal, state, county, and municipal levels, should be cognizant of the needs of the criminal justice and law enforcement community.

NJCJIS management must exercise sufficient control to comply with the interfaced operations of NCIC and NLETS. It will also manage the exchange of information statewide within the NJCJIS terminal network. The CSA will ensure that the NJCJIS terminal network is properly utilized and the exchange of CHRI, as well as other criminal justice information, is properly transacted, processed, and communicated via the various information indexes and NLETS facilities. NJCJIS management cannot vouch for the accuracy, validity, timeliness, and completeness of all information accessed and exchanged by the system users, but every effort will be made to institute and maintain a high degree of system integrity. The issue of liability has become a major consideration in the daily system usage, therefore, informed users may prove best armed to avoid litigation.

Record quality assurance, compliance with system policy and procedures, integrity, discipline, training, and proper terminal operation are essentially and ultimately the responsibilities of the individual User. Managers at all levels must ensure that available resources are committed to operational efficiency and compliance with prescribed policies and procedures. Operational assistance to the control point users is provided by the FBI/NCIC managers, the NLETS staff, and the CSA. An agency operating a computer interface, or an agency providing NJCJIS access for other agencies via its own NJCJIS terminal, will be considered a control point terminal (CPT). Assistance must further extend to the actual User, the respective terminal operator, the terminal agency coordinator (TAC), the criminal justice practitioner, the patrol officer or investigator, records personnel, the upper-level manager, and the administrator.

The rules and procedures governing direct CJIS terminal access shall apply to all other system participants as well. The User shall be bound by the rules and regulations applicable to the dissemination and use of the information obtained via NJCJIS. User agencies, whether or not equipped with CJIS terminals, shall be in full compliance when handling CHRI.

Channels utilized for the flow of timely information regarding all aspects of system usage, will consist of operating manuals and guides, newsletters, NLETS messages, and other communications. CPTs must provide the necessary descriptive operating materials for their respective system interfaces.
The purpose of this agreement is to facilitate the exchange of criminal justice law enforcement information in accordance with current laws, rules and regulations, and in compliance with operating policies and procedures applicable to authorized system participants at the federal, state, county, and municipal level. The following documents, subject matter, and procedures are incorporated by reference and made part of this agreement:

NCIC Operating Manual  NCJCIS Security Policy
NCIC Code Manual  Memorandums and other communication
NJJCIS Regulations  Department of Justice CCH
NJLETS Guide  Title 28 - Judicial Administration
NLETS Guide  Chapter 1 - Department of Justice
NJ MVC Guide  Part 20 - Criminal Justice
CCH/ANI Operating Manual  Information Systems
NJJCIS Validation  NCIC Policy Paper, December 8, 1982
Policy/Procedures Guide  Established NJJCIS policies and procedures
New Jersey Administrative Code 13:59-1.1 through 1.6  R&I Newsletters
NJJCIS Noncompliance Sanction Plan  NJWPS Operating Guide

Duties and Responsibilities Delineated. NJJCIS agrees to furnish access to the files of the NJWPS and NCIC, the communications facilities of the NJLETS and NLETS, the State Bureau of Identification's Computerized Criminal History/Automated Name Index (CCH/ANI) files, the files operated by the NJMVC and other systems or files that may be available in the future.

The Criminal Justice Information System Control Unit (CJISCU) will manage the NJJCIS computerized indexes and communications facilities at the OIT Network Control Center (NCC) located in West Trenton, New Jersey. The CJISCU will coordinate the installation of terminal hardware, software, routers, and communication lines between the OIT NCC and the User.

System availability goals are set in order to provide minimum acceptable performance. The NJJCIS computer availability goals shall be 100% with 98% as minimum acceptable performance. Local, county, and regional CPT computer availability goals shall be 100% with 98% as minimum acceptable performance. Average processing and response time shall be held in line with NJWPS/NCIC and other adopted standards.

The terminal agency administrator shall appoint a TAC to be responsible for the respective NJJCIS terminal operation. The TAC must ensure compliance with all approved policies and procedures established by the CSA.
Operational failure at the User end, within the NJCJIS terminal network, may result from one of the following four conditions:

1. the NJCJIS computer is out of service
2. router failure
3. a circuit or line problem
4. terminal equipment malfunction(s)

The User must first ensure that the failure is not associated with its equipment. Once terminal equipment malfunction has been eliminated, the OIT NCC must be contacted immediately to check circuit/line status. Any indication of circuit/line problems must be logged and furnished to the OIT NCC operator for relay to the communications vendor.

It is the responsibility of the User to contact the State Police Operational Dispatch Unit (ODU) at 609-882-2000, extension 2229, to report that the User will be out of service for any reason. The ODU will then monitor any messages directed to the out-of-service agency. The User shall also contact the ODU when service is restored. Under no circumstances should any NJCJIS equipment be disconnected or moved to another location without authorization from the CJISCU.

**NJCJIS Security Policy.** Pursuant to a security policy update, which was approved by the NCIC Advisory Policy Board on June 3, 1992, appropriate background investigations **must** be conducted on all terminal operators who access NCIC and were hired after June 3, 1992. The investigation will include completed state and federal applicant fingerprint cards submitted to the State Bureau of Identification (SBI). The New Jersey State Police has adopted this policy and expanded it to include all telecommunication systems accessed through the NJCJIS.

Procedural guidelines for conducting background investigations on prospective NJCJIS terminal operators are listed below:

1. The employing agency staff **must** check the following state and national arrest and fugitive files prior to the submission of state and federal applicant fingerprint cards:

   * New Jersey Computerized Criminal History (NJCCCH)
   * New Jersey Wanted Person System
   * NCIC Wanted Person File
   * NCIC Interstate Identification Index (III)
   * NLETS CHRI for non-III participant states
2. If a record of any kind is found, pursuant to the remote terminal checks listed above, access **will not** be granted by the employing agency. Access will be contingent upon further investigative review of arrest and/or fugitive records by the employing agency, positive identification by both FBI and SBI fingerprint comparison, and verification of the disqualifying information.

3. After positive identification of the applicant, potential disqualifying information will be forwarded to the employing agency. If the applicant is confirmed to be a fugitive from justice, or has been convicted of an indictable offense, the applicant shall be denied NJCJIS terminal operator access/certification by the employing agency.

4. Disorderly persons convictions shall not be an absolute bar to terminal operator access/certification. The agency head shall review each case and make the determination if NJCJIS access will be granted. Access shall be denied by the agency administrator if not deemed to be in the public interest.

5. Expunged records may continue to provide a disability to criminal justice employment. Pursuant to N.J.S.A. 2C:52-27c, the expunged record **may** be utilized to deny terminal operator access/certification.

6. The employing agency administrator may allow a current NJCJIS terminal operator who has been charged with an offense to remain in that capacity until resolution of the charge.

7. Police officers who are denied NJCJIS terminal operator access/certification by the employing agency are not prohibited from requesting and receiving NJCJIS record information from a certified operator in the performance of their duties.

8. NJCJIS terminal operators with convictions prior to July 13, 1994, are not subject to the disabilities outlined above. Subsequent indictable offense convictions, however, will terminate terminal access. Subsequent disorderly person convictions will be reviewed by the agency administrator to determine continued access.

9. NJCJIS management will ensure that all necessary physical site, personnel, computer, and communications safeguards prescribed are functioning properly in daily operations.
NJ CJIS USER AGREEMENT

The User shall not exchange or disseminate criminal history record information unless transactions are made in compliance with federal and state laws and approved NJ CJIS policies and procedures. The User shall ensure that all participating personnel be thoroughly informed of the federal regulations promulgated by the Department of Justice and the New Jersey Administrative Code.

Although most emphasis is placed on the security, confidentiality, and privacy of the system's criminal history information, all data exchanged or received via NJ CJIS is furnished for the exclusive use by criminal justice agencies and their authorized personnel in line with their official duties. NJ CJIS information shall not be disseminated for private or unofficial purposes.

**NJ CJIS Training Requirements.** User agencies shall comply with prescribed training requirements. Training, testing, affirmation of proficiency, and biennial retesting and reaffirmation of the proficiency of NJ CJIS terminal operators shall be the responsibility of each respective TAC. Training and reaffirmation of proficiency shall be documented and certified by the TAC.

**NJ CJIS Noncompliance Sanction Plan.** User agencies shall submit to periodic comprehensive NJ CJIS audits. Audits shall be conducted by NJ CJIS and/or FBI personnel to ensure compliance with approved policies and procedures.

NJ CJIS audits will examine training curriculum, operating procedures, validation procedures, distributed publications, supporting documentation for records, and User/Management Agreements to ensure compliance with NJ CJIS policies and procedures.

All noncompliance discrepancies will be documented and brought to the attention of the TAC and the agency administrator. If appropriate corrective measures are not implemented in a timely fashion, the three-phase NJ CJIS Noncompliance Sanction Plan will be implemented by the CSA. Sanction may result in censure, restriction of NJ CJIS access, or ultimately in termination of all NJ CJIS terminal services.

**Management Control.** In accordance with provisions set forth in the Department of Justice Computerized Criminal History Regulations, Code of Federal Regulations, Title 28, Chapter 1, Part 20, and the National Crime Information Center Policy Paper, all computers, electronic switches, and manual terminals interfaced directly with the NJ CJIS must be under the management control of criminal justice agencies. Similarly, satellite computers and manual terminals accessing NJ CJIS through a control terminal agency computer must be under the management control of a criminal justice agency.

Management control is defined as the authority to set and enforce:

1. priorities
2. standards for the selection, supervision, and termination of personnel
3. policy governing the operation of computers, circuits, and telecommunications terminals used to process criminal justice information insofar as the equipment is used to process, store, or transmit criminal justice information
Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of a criminal justice information system. Therefore, a criminal justice agency must have a written Management Control Agreement (NJCJIS 11-6) with the noncriminal justice agency operating a data center.

In addition to providing management control of a noncriminal justice agency operating a data center, the criminal justice agency administrator shall appoint a Terminal Agency Coordinator to ensure compliance with approved NJCJIS policies and procedures. New management control agreements must be executed when the administrator of the criminal justice agency or the noncriminal justice agency is replaced.

**Mobile Data Computers.** The implementation and functional use of Mobile Data Computers (MDC's), and their host central processing unit (CPU), must conform to the OIT interface protocol requirements as needed.

Prior to utilizing the MDC's, the User shall submit a letter of intent to the CJISCU which lists the number of devices and model type of each MDC. The CJISCU will assign a unique ORI to each MDC. The host CPU shall implement software to track transactions of each MDC unit and present them to NJCJIS management during agency audits. The User shall annually provide a list of MDC's and the corresponding police vehicle assignments to the CJISCU.

The User software shall restrict NJCJIS inquiry access via MDC's to the following:

1. New Jersey MVC Files
2. New Jersey Wanted Person System
3. NCIC "HOT" Files
4. NLETS RQ (vehicle registration) and DQ (drivers information) messages

Users who wish to conduct random plate inquiries (one in which the officer cannot articulate a reason for making the inquiry) must have the MVSR transaction programmed into the host CPU. An officer may only access the full disclosure inquiry (MVSP transaction) when he/she has articulable reasonable suspicion that the vehicle occupant(s) is engaged in unlawful activity.

No inquiry of any type shall be conducted based solely upon the race, ethnicity, and national origin of the occupants of the vehicle.

Police officers who are denied NJCJIS terminal access/certification, due to NJCJIS security policy disqualifiers, shall not be denied MDC system access in the performance of their duties.

The User shall be responsible for MDC system security and authorized use, i.e., MDC log-on security, password protection, and physical security to prevent theft or unauthorized access.

In the event a MDC is lost or stolen, the User shall programmatically disable the MDC from the CPU immediately. In addition, the User shall notify the CJISCU.
MDC screen formats or menus must be submitted to the CJISCU for review to ensure compliance with system policies and procedures.

Users must maintain and store the MDC transactions on disk. The disks shall be indexed, retrievable, and retained for a period of one year.

A diagnostic modem will be permitted to perform system diagnostics, network configuration checks, and vendor software maintenance under the following conditions:

1. The User’s modem shall be under the management control of the agency administrator and in a secure location.

2. The modem shall be connected only during time of actual diagnostic testing.

3. The modem line shall be equipped with quick disconnect plugs.

4. Noncriminal justice MDC maintenance personnel shall not have access to valid NJCIJS system data during diagnostic testing.

5. MDC training shall conform to the standardized requirements established by the CSA.

Agencies receiving MDC service from a host CPU operated by another agency, shall enter into a Service Agreement for Mobile Data Computers (NJCIJS 11-5B1) with the host agency.

License Plate Readers (LPR). Prior to utilizing LPRs, the User shall submit a letter of intent to the CJISCU. The CJISCU will provide the User with extracts from three NCIC Files: Stolen Vehicles, Stolen License Plates, and Wanted Persons (associated with vehicles). In addition, an extract of the NJ MVC database will be provided. The MVC information will include NJ registrations that have been suspended or expired within the last three years.

The User shall be responsible for LPR system security and unauthorized use, i.e., LPR log-on security, password protection, and physical security to prevent theft or unauthorized access.

Use of the NCIC and MVC extracts are for law enforcement purposes only.

The User shall update its local database as updates from the CJISCU become available, ensuring that information deleted from the NCIC and MVC systems are also deleted from all local databases.

Extract hits shall be confirmed in accordance with the NJCIJS hit confirmation policy.

Police Officers who are denied NJCIJS terminal access/certification, due to NJCIJS security policy disqualifiers, shall not be denied LPR system access in the performance of their duties.
NEW JERSEY DATA EXCHANGE (NJ-DEx)/NATIONAL DATA EXCHANGE (N-DEx). The NJDEx is an enhanced Search Tool which provides NJCJIS users access to shared Statewide MNI (Master Name Index) data. This repository is augmented with MNI data extracted from incident and arrest records generated by New Jersey State Police (NJSP), county Records Management Systems (RMS) and Computer Aided Dispatch (CAD) systems.

The NJ-DEx is designed to support data sharing between NJ law enforcement agencies. This process offers the ability to securely and selectively extract, share and store incident data from disparate legacy law enforcement databases across the state to support intelligence information and use as a general law enforcement tool.

Data that NJ agencies contribute to NJ-DEx will be submitted to the N-DEx. The vision of N-DEx is to enable the sharing of complete, accurate, timely, and useful information across jurisdictional boundaries and to provide new investigative tools that enhance the nation’s ability to fight crime and terrorism. N-DEx will provide law enforcement agencies with a powerful new investigative tool to search, link, analyze, and share criminal justice information such as incident/case reports, incarceration data, and parole/probation data on a national basis to a degree never before possible. N-DEx is a criminal justice information sharing system that will provide nationwide connectivity to disparate local, state, tribal, and federal systems for the exchange of information. N-DEx will allow law enforcement agencies with a powerful new investigative tool to search, link, analyze, and share information N-DEx will primarily benefit local law enforcement in their role as the first line of defense against crime and terrorism. Through N-DEx’s proposed services and capabilities, N-DEx will allow participating agencies to detect relationships between people, places, things and crime characteristics; to link information across jurisdictions; and to “connect the dots” between apparently unrelated data without causing information overload. This capability will occur primarily in the realm of structured data but can also include unstructured data. In addition, N-DEx will provide contact information and collaboration tools for law enforcement agencies that are working on cases of mutual interest. Ownership of data shared through N-DEx will remain with the law enforcement agency that provided it.

All data exchanged or received via NJ-DEx/N-DEx is furnished for the exclusive use of criminal justice agencies and their authorized personnel in line with their official duties. NJ-DEx/N-DEx information shall not be disseminated for private or unofficial purposes. The User shall be bound by the same rules and regulations applicable to the dissemination and use of the information obtained via NJCJIS as outlined in this document and the NJCJIS Security Policy.

Terms of Agreement. The terms of this agreement shall be contingent upon the availability and appropriation of funds by the State of New Jersey for the operation and maintenance of the system. Either party may cancel this agreement by giving thirty (30) days notice in writing to the other party, unless sooner terminated by casualty. NJCJIS access may also be terminated due to a security violation or by sanction. The Division of State Police shall execute and administer this agreement pursuant to the authority vested in the Superintendent.

Indemnification. The User agrees to indemnify and save harmless NJCJIS management, its employees and officials from and against any and all claims, demands, action, suit, and proceedings brought by others, and for negligence or other tortious conduct of the User, including, but not limited to, any liability
for any loss, cost, expense, and damages by reason of any claim of false imprisonment, false arrest, or any other case of action, in the exercise and enjoyment of this agreement. This agreement shall be liberally construed to apply to both types of users, those equipped with a NJCJIS terminal and those participating via another agency's terminal.

**Acknowledgement.** We hereby acknowledge the duties and responsibilities set forth in this agreement and in the documents, subject matter, and procedures incorporated by reference. We acknowledge that these duties and responsibilities have been developed and approved in order to ensure that this indispensable service be maintained along with the efficacy, integrity, and discipline considerations outlined herein. We further acknowledge that failure to comply with these commitments will subject the user agency to various sanctions outlined by the NCIC Advisory Policy Board and the NJCJIS Noncompliance Sanction Plan. These sanctions may include the termination of NJCJIS services to the User. A copy of this agreement shall be made available or be readily accessible to all participating personnel.
CRIMINAL JUSTICE INFORMATION SYSTEM
USER AGREEMENT ACKNOWLEDGEMENT

Signed as dated, the parties hereto caused this agreement to be executed by the proper officers or officials, in witness hereof. Effective date is: ________11/28/09_________.

New Jersey Department of Law and Public Safety,
Division of State Police

By: [Signature]

Title: Superintendent of State Police

Date: 11/6/09

Office of Information Technology

By: [Signature]

Title: Director

Date: 11/25/2009

Criminal Justice Agency
Agency Head/Administrator

Thomas Comey

By: [Signature] (Please Print)

Title: Chief of Police

Signature: [Signature]

Jersey City Police Department

Agency Name: 8 Erie Street, Jersey City, New Jersey 07603

Agency Address: NJ0090600

ORI Number: September 24th, 2009

Date:

All questions concerning this agreement should be directed to the NJCJS Control Unit, State Bureau of Identification, Identification and Information Technology Section, at 609-882-2000, extension 2294.

NJCJS 11-8