NON-CRIMINAL JUSTICE AGENCY USER AGREEMENT
FOR ACCESS TO CRIMINAL HISTORY RECORD INFORMATION (CORI/CHRI)
between the
MASSACHUSETTS DEPARTMENT OF CRIMNAL JUSTICE INFORMATION SERVICES (DCJIS)
and

Agency Name		
Address		
City	State	ZIP Code
Full Name and Title of Agency Head		
Telephone Number	Fax Number	
Email Address		

I. PURPOSE

This User Agreement identifies the duties and responsibilities of both the DCJIS and the non-criminal justice agency (hereinafter referred to as "NCJA" or "Agency") as they relate to the handling of requests and responses for state and national fingerprint-based criminal background checks.

The NCJA agrees to follow the terms of this agreement and will only submit requests for, review, and store CHRI background checks in accordance with 42 USC 16962, Public Law 92-544 and all other applicable federal and state laws and regulations.

II. THE PARTIES AGREE AS FOLLOWS

The DCJIS will:

1. Provide criminal history record information (CHRI) in response to submitted fingerprint-based background checks, either to the NCJA or to the appropriate agency that reviews criminal histories for the NCJA;

2. Provide assistance to the Agency in interpreting CHRI;

3. Work to ensure the completeness and accuracy of the CHRI;

4. Conduct audits to ensure compliance with this Agreement; and

5. Cease providing information to the Agency if this Agreement is violated or if the Agency is suspected of violating this Agreement.

The NCJA will:

1. Abide by the terms and conditions identified in this Agreement;

2. Abide by the terms of the current version of the FBI CJIS Security Policy (CSP) and any subsequent versions;

3. Comply with state and federal laws, rules, procedures, and policies, including those adopted by the DCJIS and the National Crime Prevention and Privacy Compact Council (Compact Council) regarding the use and dissemination of CHRI;

4. Use CHRI only for the purpose requested;

5. Submit requests for CHRI checks only as authorized by law;

6. Provide for the security of any criminal history record information received. This includes, but is not limited to:

    a. designating a Local Agency Security Officer (LASO) who is responsible for ensuring compliance with security procedures and this User Agreement.
    b. ensuring all personnel with access to CHRI are aware of the rules and responsibilities with regard to CHRI and have completed the required training.
    c. restricting access to physical or electronic copies of CHRI to authorized personnel. Physical copies shall be maintained in a controlled, secure environment, such as a locked cabinet in a room not accessible to all staff and visitors. Electronic copies shall be protected with at least 128-bit encryption. The relevant federal encryption standard is FIPS 140-2.
    d. sharing CHRI only when explicitly allowed by law and logging any CHRI dissemination. Logs shall include, at a minimum, the subject's name, the subject's date of birth, the date and time of dissemination, the name of the person to whom the CHRI was disseminated along with the name of the organization for which the person works, and the specific reason for dissemination.
    e. tracking and reporting information security incidents, such as the theft/loss of physical records or the penetration of electronic systems.
    f. disposing of CHRI in the required, secure manner. Physical media must be cross-shredded and/or burned, and electronic records must be deleted and repeatedly over-written with random 0s and 1s, or the media must be degaussed.

7. Understand this data is based on CHRI received by the DCJIS. If a person could be adversely affected by this data, the person must be given the opportunity to challenge and correct a record before a final decision is rendered on the basis of the CHRI;

8. Retain audit records for at least 365 days. Once the minimum retention time period has passed, the agency shall continue to retain audit records until they are no longer needed for administrative, legal, audit, or other operational purposes;

9. Allow the DCJIS and the FBI to conduct audits to ensure compliance with this Agreement; and

10. Respond to, and cooperate with, the investigation of any complaints alleging a violation of this agreement or of the laws, regulations, and policies regarding access to, and use of, CHRI information.

III. CRIMINAL HISTORY RECORD INFORMATION LIMITATIONS

The NCJA understands that CHRI has the following limitations:

1. CHRI is based solely upon arrest fingerprint cards submitted to the Massachusetts State Police (MSP) State Identification Section (SIS) and to the FBI. The arrest warrant file, sex offender file, or other databases maintained by the DCJIS are not part of the CHRI search.

2. CHRI is compiled from information submitted to the MSP SIS and to the FBI by law enforcement agencies (hereinafter referred to as contributing agencies). Although the MSP SIS makes reasonable efforts to ensure all information is submitted as required by State law, it is not responsible for omissions from contributing agencies.

3. Although the MSP SIS encourages the reporting of all arrests for felony, misdemeanor, and drug violations, Massachusetts law enforcement agencies are only required to submit fingerprints on felony and drug-related arrests.

4. CHRI is constantly being updated as new arrests and other information are entered into the system by contributing agencies. The record released is only valid as of the date the record check was performed.

5. Certain statutes allow for the suppression or deletion of records, and this information is not provided.

6. The MSP SIS retains records for the State of Massachusetts only. Most fingerprint-based background checks include a check through the FBI, which the MSP SIS will request on the NCJA's behalf as a normal part of the criminal background check, if allowed by law.

IV. PERSONNEL SECURITY AND TRAINING REQUIREMENTS

Individuals within the NCJA who have direct access to CHRI or to systems containing CHRI are subject to criminal history record checks performed by the DCJIS. The NCJA agrees to ensure that all affected personnel are screened as provided in this agreement.

Access will be denied if the individual has ever had a felony conviction of any kind, no matter when it occurred. Access may be denied if the individual has one or more recent misdemeanor convictions. In addition, an individual believed to be a fugitive from justice, or having an arrest history without convictions, will be reviewed to determine if access to CHRI is appropriate. The DCJIS will take into consideration extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

In addition to the above, CHRI access will be discontinued for any person who is subsequently arrested for, or convicted of, a crime. The NCJA's Local Agency Security Officer (LASO) must report such incidents to the CJIS Systems Officer at the DCJIS for review before access may be reinstated. The NCJA further agrees that where authorized by law, support personnel, contractors, vendors, and custodial workers with access to controlled areas during CHRI processing will undergo state and/or national criminal background checks unless escorted by authorized personnel at all times.

The LASO will be responsible for reporting all personnel security clearance requests and issues to the DCJIS CSO within five (5) business days.

An informed review of CHRI results requires training. As such, the NCJA agrees that all authorized personnel, including those personnel with direct access to SAFIS-R and those that will access SAFIS results, will complete the required training and review all training materials made available by the DCJIS every two years. Furthermore, all authorized personnel must also execute a Criminal Record Information (CORI/CHRI) Individual Agreement of Non-Disclosure (AOND) form.

V. PHYSICAL AND ELECTRONIC SECURITY OF CHRI

The NCJA is responsible for ensuring the physical and electronic security of CHRI at all times. Therefore, the NCJA must adhere to the following:

1. CHRI shall only be processed in controlled areas with limited access.
2. Computers which provide access to CHRI data shall not be logged in when unattended.
3. Authorized users shall not share Usernames and Passwords.
4. Documents shall not be left out in the open as they could be viewed by unauthorized individuals.
5. Computer screens and CHRI shall not be viewable by unauthorized individuals.
6. File cabinets and record rooms shall be locked when unattended.

VI. INCIDENT RESPONSE REQUIREMENTS

A "security incident" is defined as (a) unlawful or unauthorized access to, and/or dissemination of, any CHRI stored on the NCJA's equipment or in the NCJA's facilities resulting in access to, or loss, disclosure, or alteration of, CHRI, or (b) unlawful or unauthorized access to such facilities or equipment resulting in access to, or loss, disclosure, or alteration of, CHRI.

The NCJA LASO shall report any and all security incidents to the DCJIS Information Security Officer (ISO) within 48 hours of the discovery of the incident.

VII. DOCUMENT SIGNOFF

This Agreement commences on the date the last signature is obtained below and continues until terminated by one of the parties. Written notice of one of the parties' intent to terminate this agreement must be submitted at least 14 days prior to the termination date. This Agreement may be terminated sooner by the DCJIS upon a violation of the terms of the Agreement.

NON-CRIMINAL JUSTICE AGENCY

Signature of Agency Head	Date
Title	
Print or Type Name	

MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

Signature of CJIS Systems Officer, DCJIS	Date
Print or Type Name Jamison R. Gagnon	

Submit the completed Agreement via U.S. Mail or via email to:

Massachusetts Department of Criminal Justice Information Services
ATTN: SAFIS Unit
200 Arlington Street, Suite 2200
Chelsea, MA 02150
Telephone: 617.660.4790
Email: safis@mass.gov