CONSOLIDATED RECORDS MANAGEMENT SYSTEM

(CRMS) USER AGREEMENT

I. PURPOSE STATEMENT

The TENNESSEE FUSION CENTER (TFC) is an initiative of the Tennessee Bureau of Investigation (TBI) and the Department of Safety and Homeland Security, with the goal of providing resources, expertise, and information in order to maximize the ability to detect, prevent, investigate, and respond to criminal and terrorism activity. As part of the TFC, the Consolidated Records Management System (CRMS) was established to provide timely information sharing and exchange of crime-related information among members of the law enforcement community. The CRMS is a database repository containing criminal incident/offense records, and other law enforcement activity records, submitted and updated by law enforcement agencies and criminal justice organizations into the CRMS; this includes additions, updates, or deletions of records as submitted by the originating agency. CRMS records are not Criminal Intelligence Information and as such, are not governed under 28 CFR Part 23. This product and service is made available to law enforcement agencies and other entities contributing to public safety throughout the state and country.

The goal of this project is to provide computer mechanisms in the form of network connectivity, hardware and software, necessary for public safety agencies and emergency responders to provide information to and query information in the Consolidated Records Management System (CRMS). Participating agencies will share incident based information components and suspicious activity reports for replication or entry of information to the CRMS and will have the capability to query all CRMS information from around the state which is stored within the CRMS warehouse. Lessons learned through this project will be shared nationally through the National Institute of Justice, Office of Science and Technology.

II. DEFINITIONS

"Fusion Center": the operations center consisting of analysts, and other supervisors; synonymous with the TFC.

"Governance Board": the management body overseeing the direction of the Tennessee Fusion Center.

"Requestor": the individual law enforcement officer or agency making a request for information from, or reporting an incident to, the Fusion Center; synonymous with "user."

"Reasonable Suspicion/Criminal Predicate": when sufficient facts and or circumstances are established to give a trained law enforcement officer or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise per 28CFR23.

"Personal Data": any information relating to an identifiable individual.

III. DATA QUALITY

The CRMS is maintained for the purpose of developing information and intelligence for and by participating stakeholder agencies. The decision of the agencies to participate with the fusion center and to decide which databases to provide for fusion center access is voluntary and will be governed by the laws and rules governing those individual agencies, as well as by applicable federal laws.

Agencies participating in the fusion center and providing data to the CRMS remain the owners of the data contributed and are responsible for the quality and accuracy of the data. Any information obtained through the CRMS should be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

IV. USE LIMITATION

Information obtained from or through the CRMS can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a possible criminal act or threat to public safety.

The TFC Governance Board or designee will take necessary measures to ensure access to the fusion center's information and intelligence resources is secure. Unauthorized access or use of the resources is forbidden. The Board reserves the right to restrict the qualifications and number of personnel having access to the fusion center and to suspend or withhold service to any individual or agency violating this *Agreement*. The Board, or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the fusion center.

All personnel who receive, handle, or have access to CRMS data will be limited to those individuals who have been selected, approved, and trained accordingly. All personnel having access to CRMS data agree to abide by the following rules:

1. CRMS data will be used only in support of official law enforcement or public safety activities in a manner authorized by the requestor's employer.
2. Individual passwords will not be disclosed to any other person.
3. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
4. Participating agencies will ensure users have the legal authority to access criminal incident/records.
5. Use of the CRMS data in an unauthorized or illegal manner will subject the requestor to denial of further use of the CRMS, discipline by the requestor's employing agency, and/or criminal prosecution. (see CRMS Sanctions Policy).

The TFC reserves the right to deny access to any CRMS user who fails to comply with the applicable restrictions and limitations of the CRMS Agreement and that user will be subject to the CRMS Sanctions Policy.

V. SECURITY

Information obtained from or through the CRMS will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding signed with the participating agency. Information cannot be:

- sold, published, exchanged, or disclosed for commercial purposes;
- disclosed or published without prior approval of the contributing agency; or
- disseminated to unauthorized persons.

Access to the fusion center's databases from outside of the facility will only be allowed over a secure network. Research of the CRMS data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the CRMS will be granted only to fully authorized personnel who have been selected by the agency Chief Executive Officer.

VI. OPENNESS

CRMS data can be requested from the originating agency at any time by the public. It is the responsibility of the originating agency to comply with applicable State and Federal law in responding to any such request. All requests for information contained in CRMS from the public will be referred to the originating agency as appropriate. The TFC will post this *Agreement* on its web site and make it available to any interested party.

VII. INDIVIDUAL PARTICIPATION

The data maintained by the CRMS is obtained through participating stakeholder agencies. Individual users of CRMS information are solely responsible for the interpretation of that information developed in the research process. Additionally, it is the responsibility of the user to ensure the accuracy, validity, and completeness of all information and or intelligence obtained prior to official action being taken in full or in part.

Members of the public cannot access personal information for themselves or others from the fusion center applications. Persons wishing to access personal data pertaining to themselves should communicate directly with the agency or entity responsible for the data in question. Participating agencies agree that they will refer requests related to privacy back to the originator of the information.

Further dissemination and use of information obtained from the CRMS will be utilized in accordance with originating source use restrictions and applicable policy.

VIII. ACCOUNTABILITY

Queries made to the CRMS will be documented identifying the user initiating the query within CRMS. The TFC Governance Board or its designee will be responsible for conducting or coordinating internal or special audits, and for investigating misuse of the fusion center's information systems. All confirmed or suspected violations will be reported through the TFC Chain of Command to the Governance Board. Individual users of CRMS information remain responsible for the appropriate use of the information. Each user of the CRMS and each participating agency within the TFC are required to abide by this *Agreement*. Failure to abide by the restrictions for the use of the CRMS data may result in the suspension or termination of user privileges (see CRMS Sanctions Policy); discipline imposed by the user's employing agency, or criminal prosecution.

TNCOP/CRMS SANCTION POLICY

1. Sanction violations include, but shall not be limited to, the following:

    a. Computer security violations resulting in the disclosure of sensitive or classified information to unauthorized individuals or the accessing of TnCOP/CRMS information inappropriately and/or for unauthorized purposes.

    b. Any activity that results in unauthorized modification or destruction of system data, loss of computer system processing capability or loss by theft or any computer media including but not limited to memory, optical or magnetic storage medium, hardcopy printouts, etc.

2. When discrepancies are discovered at the agency, they must be documented and reported to the Agency Administrator and the RMS Administrator. The incident shall then be reported in writing to the TBI CJIS Support Center (CSC), along with any disciplinary action that was taken.

3. When non-compliance issues are discovered by the TBI CSC, they will be documented and reported to the Agency Administrator and RMS Administrator.

4. If an authorized user is found to be in noncompliance, the CSC will:

    a. Forward the investigation results to the head of the authorized user's employing agency;

    b. Suspend or discontinue access to information by the authorized user, if necessary, until a determination regarding appropriate disciplinary measures, if any, are made by the employing agency under any applicable preferred service rules or other state or federal laws or regulations regarding the authorized user's employment;

    c. Cooperate with the applicable agency in any disciplinary action and/or hearing as may be necessary; and,

    d. Refer the matter to appropriate authorities for criminal prosecution, as necessary.

5. If a participating agency is found to be in noncompliance, the Tennessee Fusion Center (TFC) will:

    a. Forward the investigation results to the Director of the CSC and the head of the participating agency;

    b. Suspend participating agency access or terminate the MOU, if necessary, based on the severity of noncompliance; and,

c. Refer the matter to appropriate authorities for criminal prosecution, as necessary.

6. All infractions will be documented and reported to the Agency Administrator and the RMS Administrator for review and immediate corrective action. A written formal response from the Chief Law Enforcement Officer (CLEO) shall be forwarded to the Director of the CSC within thirty (30) days of the agency being found to be in a non-compliance status. The following issues shall be addressed:

   a. Non-compliance issues cited;
   b. Documentation of corrective measures;
   c. Agency's plan to eliminate future non-compliance; and
   d. Documentation of retraining of agency personnel, if applicable.

7. Where non-compliance remains an issue after thirty (30) days, the following will occur:

   - A letter from the Director of the CSC will be forwarded to the CLEO/Administrator, with a copy forwarded to the TBI Director, and other governing administrators. This letter will outline the infractions that lead to the imposed sanctions:
   - The following limited sanctions will be imposed:

     a. Access to the TnCOP/CRMS system will be suspended for sixty (60) days;
     b. The agency will be placed on sixty (60) days probation; and
     c. If the agency uses TnCOP as their sole TIBRS reporting software, one account will remain active for the purpose of uninterrupted reporting. The CSC will make a determination as to the person who will be provided the account information.

8. If non-compliance remains an issue at the conclusion of the sixty (60) day probationary period, additional sanctions will be enacted as detailed below:

   - A formal letter from the Director of the CSC will be forwarded to the CLEO/Administrator, the CSO, and other governing administrators. The letter will address the non-compliance issue(s), failure to carry out corrective measures, and previously imposed sanctions. Copies of all correspondence to the agency concerning non-compliance will be included.
   - The following limited sanctions will be imposed:

     a. The CSC will cancel all TnCOP/CRMS services to the agency;
     b. The participating agency MOU agreement will be suspended; and
     c. After six (6) months of terminated service, the agency may formally request reinstatement of TnCOP/CRMS services.

9. To regain access to suspended TnCOP/CRMS services, a formal letter from the agency's CLEO/Administrator must be submitted to the Director of the CSC. The following issues must be addressed:

a. Non-compliance issue(s) that initiated the enforced sanctions;
b. Corrective action taken by the agency's CLEO/Administrator;
c. Implemented plans to ensure future compliance; and
d. Documentation of retraining agency personnel.

10. The agency will be placed on probation for one year after TnCOP/CRMS services have been reinstated.