



KANSAS CITY MISSOURI POLICE DEPARTMENT

PROCEDURAL INSTRUCTION

DATE OF ISSUE

04/08/2015

EFFECTIVE DATE

04/08/2015

NO.

15-06

SUBJECT

Computerized Police Information Systems

AMENDS

REFERENCE

REJIS, MULES and NCIC System Manuals, RSMo Chapter 610

RESCINDS

PI 01-10
DM 12-4**I. PURPOSE**

To establish Department policies and procedures with respect to collection, ethical use, and any subsequent release or exchange of information available through the Criminal Justice Information Systems (CJIS).

II. POLICY

- A. Department of Justice directive, Criminal Justice Information, Title 28, and the Code of Federal Regulations, Part 20, are recognized as the governing directives for CJIS.
- *B. All information released to the public must adhere to RSMo 610 (Sunshine Law), CJIS rules and other applicable state and federal laws and regulations.
- C. When it becomes apparent that computer technology can be utilized to increase the efficiency and/or effectiveness of police operations, such technology will be applied, provided that resources can be made available.
- *D. To ensure that the Department is in compliance with CJIS rules and State Statutes, department members will not include criminal history information in case files submitted to any prosecutors' office. Members of the prosecutors' offices have received the proper training and may access criminal history information for criminal justice purposes. Department members will not make any secondary disseminations of criminal history information.
- *E. Certification and Security Awareness Requirements
 - 1. Basic security awareness training shall be required, within six months of initial hire and every two years thereafter, for all personnel who have access to criminal justice information (CJI). Three levels of security awareness training will be presented depending on the type of access a person has to CJI.
 - a. Level 1 – Individuals who have access to CJI, but do not have personal system access. Example: Officers who do not have MDC access.
 - b. Level 2 – Operators with logical access to CJIS systems. Example: Operators in 911/dispatch centers or records units.

- c. Level 3 – Technical personnel with programming or configuration access to CJIS systems. Example: Technical and support personnel with responsibility for maintaining hardware and network.
2. Operators and support personnel who have direct system access will receive security awareness during their initial Missouri Uniform Law Enforcement System (MULES) training and recertification.
 3. Individuals who have access to CJI may receive security awareness training from other sources, such as materials provided by the Missouri State Highway Patrol (MSHP) CJIS Security Unit or through cjisonline.com.
 4. New operators may be granted provisional access at the level they will ultimately be certified for. Operators must complete all appropriate certification training within six months of appointment to a terminal operator position.
 - a. If an operator fails to complete training sufficient for their level of access within six months, they will be reduced to restricted access until certification is completed.
 - b. During the provisional access period, the new operator must be under the direct or very close supervision of an operator certified for at least the same level of access as the provisional operator until a basic level of proficiency is met.

*F. Recertification

1. All operators with full access must recertify every two years and attend a one-day certification course presented by a member of the CJIS training staff.
2. Operators with inquiry access must complete security awareness training every two years.
3. Inquiry access operators have the option of taking an online recertification test via the NexTEST system.

*G Direct access to computerized criminal justice information will be restricted to criminal justice agencies (Records Management System (RMS) Corrections Management System (CMS) etc.). Requests for access to other types of information in the computer system will be reviewed on an individual basis.

1. Use of CJIS for personal use is prohibited.

2. Data stored within the system will be limited to that information which is based on or contained in source documents maintained on file in the agency or element responsible for the action contained in such document.
3. Under no circumstances will unauthorized persons be given a copy of a computer printout that contains criminal history record information, nor will members verbally release this information to such persons. Those individuals who utilize computerized information must understand that careless or unethical use of such data represents unprofessional conduct that may result in disciplinary action and/or legal sanctions.
4. Members will take every precaution to prevent unauthorized persons from obtaining information from a computer display or printout.
5. Criminal History Records Information (CHRI) may be e-mailed if the email network being used meets the security requirements set forth in the CJIS security policy. Under no circumstances will e-mails be sent outside the domain from which they originate, which means that the part of the address after the "@" must match for both sender and recipient. E-mails in which the address domains change are not secure, even if each individual system is secure.
6. When computer printouts, investigation reports, etc., are no longer needed, they will be shredded to prevent disclosure of the information contained therein to unauthorized persons.
7. The computerized information system will be designed to exclude inquiries inconsistent with system rules.

*H. CJIS Inquiries

1. All personnel regularly assigned to positions requiring computer terminal operations and requiring access to the Regional Justice Information Service (REJIS) will familiarize themselves with the REJIS, Missouri Uniform Law Enforcement System (MULES), National Crime Information Center (NCIC) and terminal equipment manuals, and will become proficient in terminal operation.
2. All inquiries to the REJIS System will require the terminal operator to use a numeric identifier for identification of the requesting member. This applies to all systems (e.g., inquiries, record checks, registration checks, etc). This excludes members who utilize special programs on the mainframe (such as INTELLECT) and are required to enter a password.
 - a. Dispatchers will use the requesting officer's radio number for requests via radio.

- b. Under no circumstances will a member's User ID and password be shared.
- 3. Station personnel will be responsible for ensuring that all persons arrested and booked have been computer checked prior to release.
- *I. The Kansas City, Missouri Police Department is responsible to MULES and NCIC for security and discipline of computer operations in order to maintain the integrity of both systems. Any violation of such security will be investigated and disciplinary action may be taken for any policy violations.
 - 1. Information exchanged over the NCIC network involves official FBI and other criminal justice agency information and will be considered privileged.
 - 2. Such information will be processed and safeguarded in such a manner that only personnel involved with official criminal justice business will have access to it.
- *J. All requests for historical data retrieval (log dump) should be forwarded to the Information Services Division Commander or their designee.

***III. PROCEDURE**

This procedural instruction has been arranged in annexes to address the various areas of concern, which are pertinent to the use of the CJIS. The provided procedures are not all inclusive. The user may find it beneficial or necessary to reference other relevant procedural instructions or REJIS, MULES, or NCIC System Manuals.

- Annex A Terminology
- Annex B Transport/Storage/Disposal of Records
- Annex C Criminal History Record Information (CHRI)

Darryl Forté
Chief of Police

Adopted by the Board of Police Commissioners this ___ day of _____, 2015.

Alvin Brooks
Board President

DISTRIBUTION: All Department Personnel
Public View Master Index - Internet
Department Master Index - Intranet
Policy Acknowledgement SyStem (PASS)

TERMINOLOGY

- A. **Alias** – Either the first, last, or both names of a subject, which are not his/her true names. An example would be John Doe, alias: John Roe, Robert Doe, or Robert Roe. The addition, deletion, or changing of a middle initial does not constitute an alias.
- B. **Armed** – A subject, who has been known to be in physical possession of a dangerous weapon, and has been arrested in connection with a violent criminal act where a dangerous weapon was used.
- C. **Arrest** – The custodial apprehension of a person upon probable cause to believe the suspect has committed a felony, misdemeanor, or ordinance violation.
1. **Charged** - The initiation of formal (written) adversary judicial proceedings against a person accused of a law violation, i.e., complaint, information, or indictment.
 2. **Released** - Not held in custody.
- D. **Cancel** (NCIC, MULES) – Remove from files immediately; information was either entered erroneously or is no longer accurate.
- *E. **Caution Indicators** – Indicators located within the MULES system which alert law enforcement officers to potentially dangerous individuals. These caution indicators are as follows:
- Caution-1**-Known to be violent.
- Caution-2**-Known to be armed.
- Caution-3**-Known to have assaulted or obstructed a peace officer.
- F. **Clear** (NCIC, MULES) – Remove from files; person/property/vehicle has been apprehended or recovered and no longer requires a stolen/wanted status.

- G. **Criminal Justice Agency** – Any agency having primary responsibility for the administration of criminal justice and which allocates in excess of 51 percent of its budget for this purpose in one or more of the following categories:
1. Arrest and/or prosecution.
 2. Adjudication.
 3. Administration of probation and/or parole.
 4. Detention of subjects in the criminal justice process.
- *H. **CJIS Network** – Entire network of terminals, circuits, computers, etc., connected to the MSHP computerized systems. It also includes all systems that interface with MULES, including NCIC, International Justice and Public Safety Network (NLETS), Missouri Department of Revenue (DOR), Traffic Arrest System/DWI Tracking System (TAS/DWITS) and all files maintained by these systems, such as stolen vehicles or property, wanted and missing persons, and registered sex offenders.
- *I. **Criminal Justice Information (CJI)** – Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:
1. **Biometric Data** – Data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population and used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
 2. **Identity History Data** – Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
 3. **Biographic Data** – Information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
 4. **Property Data** – Information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

5. Case/Incident History – Information about the history of criminal incidents.
- *J. **Criminal History Record Information (CHRI)** – Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, and release.
- K. **Dangerous** – A person who has exhibited a harmful or violent physical action toward other people, including law enforcement officers.
- L. **DOR** – A computer information system in Jefferson City, Missouri, which maintains the Missouri driver and motor vehicle files.
- *M. **Electronic Media** – Any electronic storage media including memory devices in laptops and computers and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, digital memory card, or other such devices.
- N. **Hit** – Any response to a computer inquiry other than "Not on File" or its variations.
1. Negative – A hit which is determined to be on some person or object other than the one on which an inquiry was made.
 2. Positive – A hit which is determined to be on the person or object on which an inquiry was made, indicating the person may be wanted or the property stolen/lost.
- O. **III** – (Interstate Identification Index or Triple I) – A file maintained by NCIC which provides an index of all fingerprinted offenders filed with the Federal Bureau of Investigation (FBI) and the states holding the detailed rap sheets.
- P. **Law Enforcement Agency** – A criminal justice agency dealing with arrest and/or prosecution.
- Q. **Locate Message** – Indicates a temporary change in record status in the NCIC and/or MULES files. The message is sent by the agency locating a person or property previously entered by another agency.
- *R. **MULES** (Missouri Uniform Law Enforcement System) – Missouri's law enforcement computer network. MULES provides relay for law enforcement information and message traffic, and houses files on people, vehicles, or property of interest to law enforcement.

- S. **NCIC** – The National Crime Information Center is maintained by the FBI's CJIS Division.
- *T. **NLETS** – A private, not-for profit interstate criminal justice and public safety information sharing network.
- *U. **Records** – Any document, book, paper, photograph, sound recording, video recording, or other material, regardless of physical form or characteristic, including electronic, made or received pursuant to law or in connection with the transaction of official business. The record that is kept on file is subject to the requirements of the retention schedule. The record must be listed on the disposal form upon destruction. This definition includes those records created, used and maintained in electronic form.

TRANSPORT/STORAGE/DISPOSAL OF RECORDS

- A. While in transit, members will place records in an envelope or folder. The envelope or folder will be sealed with evidence tape in such a manner that any possible opening or tampering with the contents will not go unnoticed. The minimum required information for a seal includes the member's initials, serial number, case report number and date in order to maintain the integrity of the evidence.

- B. When computer printouts are no longer needed, they will be shredded to prevent disclosure of confidential information contained therein to unauthorized persons.
 - 1. Shredders or shredder barrels are available at various locations throughout the Department.

 - 2. Commanders will designate a specific area where the shredder will be placed. When applicable, a container marked "Material To Be Shredded" will be placed next to the shredder where members may place discarded printouts, reports, etc.

 - 3. The Building Operations Unit is responsible for the maintenance of the barrels. Any unit desiring a barrel will contact Building Operations.

 - 4. All other locations will transport material for shredding to the nearest shredder location or contact Building Operations Unit for pick-up of large quantities.

- *C. All electronic media will be sanitized prior to disposal or release for reuse by unauthorized individuals.
 - 1. Written documentation of the steps taken to sanitize or destroy electronic media shall be maintained.

 - 2. The sanitization or destruction shall be witnessed or carried out by authorized personnel from the Information Technology Unit (ITU) or their designee.

CRIMINAL HISTORY RECORD INFORMATION (CHRI)

- A. To ensure the security and integrity of CHRI, department members will conform with state and federal laws and regulations regarding the release of criminal history record information. Members are cautioned that unauthorized release of criminal history record information is a violation of state and federal law and may result in criminal penalties and/or disciplinary action.
- B. Criminal history records of the Kansas City, Missouri Police Department will be generally categorized as arrest reports, incident reports and investigative reports. This information will be collected, stored, and released outside the department and destroyed in strict conformance with state statute and federal regulations.
- C. CHRI may be released from the Department only via the Information Management Unit, OGC, Criminal Records Section, Identification Section, or division station desk personnel. Copies of record information will be furnished only under special procedures established by the Information Management Unit. Other members will not release any criminal history record information to a non-department member, except for specific investigative purposes authorized by law.
- D. Non-conviction CHRI (closed record) is inaccessible to the general public and to all persons other than the defendant, except as provided in Section 610.120 RSMo. The decision as to whether any record will be deemed to be closed under the provisions of Section 610.100.3 RSMo, will be at the discretion of the Chief of Police or his designee. Non-conviction CHRI will not be revealed except as outlined below:
 - 1. To individuals for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order, if any.
 - 2. To department members for investigation and prosecution purposes in conformance with Section 610.100 and 610.120 et. Seq. RSMo. 1989.
 - 3. To courts, law enforcement agencies, and federal agencies for purposes of prosecution, sentencing, parole consideration, criminal justice employment, child care employment, and nursing home employment; and to federal agencies for investigative purposes authorized by law or presidential executive order.
 - 4. To the individual named in the record, upon request.

5. In response to a specific inquiry about a matter of public record, not otherwise prohibited by regulation or statute.
 - a. If a person is arrested but not charged within thirty days of arrest, state law requires that such records be closed.
 - b. If the person arrested is charged but subsequently not convicted, state law requires that such records be closed.
 - c. State law (Section 211.321 RSMo. 1980) prohibits release of any CHRI regarding juveniles. All requests for juvenile CHRI should be referred to OGC.
 - d. Federal regulation requires that any authorized release of criminal history record information to non-criminal justice agencies or individuals be limited to the specific purpose for which it is given.
6. Mug shots or photographs of suspects in criminal cases, which are taken as a part of an arrest, will be deemed to be a part of the arrest record and will be made available to the public in accordance with the requirements of Missouri law as to arrest records. Other mug shots and photographs will be deemed to be a part of investigative records and will be made available to the public in accordance with the requirements of Missouri law as to investigative records.
7. Citizens who request CHRI about themselves will be requested to respond to the Criminal Records Section or a division station. The Information Management Unit Commander or designee has the discretion to correct any disputed record, or forward the challenge to the General Counsel who will determine if the record will be amended.
8. Records, files, and documents compiled in the course of completed criminal investigations will be open records, except as otherwise provided for in any applicable Board of Police Commissioners Resolution, written directive, court rules, and case law concerning the prosecution of criminal cases.
9. Members of the news media will be treated as any other private inquirer. Information regarding current investigations will be released in accordance with the current written directive entitled, "Media Contacts and Interactions."

10. Private security officers and private security companies will be treated as any other member of the public seeking information. They will not be provided with non-conviction criminal history record information for employment checks or other purposes, except as provided for in applicable written policy.
11. Unauthorized government or public agencies (those agencies not identified by statute) will be treated as any other private inquirer, unless they can provide legal authorization for release of criminal history record information. Non-conviction information for non-specified employment checks or other purposes will not be released without such authorization.
12. Attorneys requesting to see criminal history record information regarding a client may be referred to the department OGC for approval. Upon determination that the request is legitimate, the OGC will notify the Criminal Records Section supervisor.
13. Whenever a criminal background check is requested in connection with gaining employment, housing or any other services or benefit of any homeless, honorably discharged, member of the organized militia or the armed forces of the United States, such background check or copy of any relevant public record will be completed and transmitted to the requesting party without any fee or other compensation. (Section 610.103 RSMo).
14. If doubt exists regarding the lawful and proper release of criminal history record information, the matter will be referred to the Information Management Unit Commander, his/her designee, or the OGC.
15. All requests for records not specifically provided for herein will be referred to the OGC, who will determine if the records requested are open or closed records, and if the same should be released.
16. In accordance with the provisions of Section 610.026 of the Revised Statutes of Missouri, a reasonable fee will be charged for all records released by the Kansas City Missouri Police Department.
17. Warrants are public information unless the warrant was issued 'under seal' by the court. If under seal, neither the record of the warrant nor existence of the warrant will be revealed.