KANSAS CITY MISSOURI POLICE DEPARTMENT **PROCEDURAL INSTRUCTION**	DATE OF ISSUE 7/1/2020	EFFECTIVE DATE 7/1/2020	NO. 20-07
SUBJECT Computerized Police Information Systems		AMENDS	
REFERENCE PI Personally Identifiable Information (PII), Criminal Justice Information Systems (CJIS), Missouri Uniform Law Enforcement System (MULES) and National Crime Information Center (NCIC) System Manuals, RSMo Chapter 610, 28 CFR part 20		RESCINDS PI 15-06 DM 11-2; 12-11	

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 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. Any member that becomes aware of a breach or imminent breach of Personally Identifiable Information (PII) will immediately notify the Information Technology (IT) helpdesk. The IT help desk will then immediately contact the Local Area Security Officer (LASO) and the Grant Administrator at **[REDACTED]**. For further information refer to the current written directive entitled, “Personally Identifiable Information (PII).

D. 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.

*E. 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, unless a signed user agreement is in place. Department members will not make any secondary disseminations of criminal history information.

*F. 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 – Personnel with unescorted access to a physically secure location. This level is designed for people who have access to a secure area but are not authorized to use CJI.

b. Level 2 – All personnel with access to CJI. This level is designed for people who do not have physical and logical access to CJI but may encounter it in their duties.

c. Level 4 – Personnel with information technology roles. This level is designed for all information technology personnel including system administrators, network administrator, etc.

2. Operators and support personnel who have direct system access will receive security awareness during their initial MULES training and recertification.

3. Individuals who have access to CJIS 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. Prior to being certified, new operators may be granted provisional access. 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.

G. 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. When inquiry operators recertify online the security awareness training is included.

3. Inquiry access operators have the option of taking an online recertification test via the NexTEST system.

H. Direct access to computerized CJI 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.

I. CJIS Inquiries

1. All personnel regularly assigned to positions requiring computer terminal operations and requiring access to the CJIS will familiarize themselves with the CJIS, MULES, NCIC and terminal equipment manuals, and become proficient in terminal operation.

*2. All inquiries to the CJIS System will require the terminal operator to use a unique 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.

J. The 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.

K. 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 CJIS, MULES, or NCIC System Manuals.

Annex A Terminology

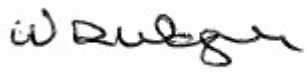
Annex B Transport/Storage/Disposal of Records

Annex C Criminal History Record Information (CHRI)

*Annex D NCIC Requirements for Criminal History Inquiries

Richard C. Smith
Chief of Police

Adopted by the Board of Police Commissioners this 16th day of June, 2020.



W. Don Wagner
Board President

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

ANNEX A

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) adversarial 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 therefrom, 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. **Department of Revenue (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. **Interstate Identification Index or Tripple I (III)** – A file maintained by NCIC which provides an index of all fingerprinted offenders filed with the 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'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** –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. **Record** – 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.

ANNEX B

TRANSPORT/STORAGE/DISPOSAL OF RECORDS

*A. While in transit, members will place records in an envelope or folder.

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 Unit.

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 Systems Unit (ITU) or their designee.

ANNEX C

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 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, Office of General Counsel (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.

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 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. 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.

8. 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.”

9. 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 directives.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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 Department.

15. 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.

ANNEX D

*NCIC REQUIREMENTS FOR CRIMINAL HISTORY INQUIRIES

A. When members complete a transaction for criminal history inquiries, the following authorized purpose codes will be used:

1. **Purpose Code C (Criminal Justice)--**Used in connection with the administration of criminal justice. The following examples provide clarification for authorized uses of this code in situations that are not part of a criminal justice investigation but are duties of the agency where a criminal record check is necessary to accomplish the agency's mission. These examples are not all encompassing.

   a. Vendors or contractors at criminal justice agencies who are not involved with the actual administration of criminal justice; e.g., carpet cleaners, individuals responsible for maintaining vending machines, janitors, and cooks.

   b. Volunteers at criminal justice agencies who are not involved with the actual administration of criminal justice; e.g., volunteers at a confinement facility who are providing social or community services rather than rehabilitative services.

   c. Confinement facility visitors, e.g., jail tours.

   *d. Inmates of a confinement facility.

   e. Participants attending and handling firearms during a law enforcement-sponsored firearms training class held at a public firing range or law enforcement facility.

2. **Purpose Code F (Weapons-Related Background Checks)--**Used by criminal justice agencies for returning firearms to their lawful owners and enforcing federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned.

3. **Purpose Code J (Criminal Justice Employment)--**Unless restricted or prohibited by state statute, state common law, or local ordinance, this code is used when the transaction involves employment with a criminal justice agency or the screening of employees of other agencies required to have management control.

Such screening may include the use of the criminal history background checks of friends, relatives, and associates of the employee or applicant. This code is used for initial background checks of agency personnel, as well as the following:

a. Non-criminal justice agencies involved with the administration of criminal justice on behalf of the criminal justice agency.

b. Volunteers at the criminal justice agency who are involved with the administration of criminal justice, e.g., volunteer dispatchers, volunteer data entry clerks, volunteers at a confinement facility who are providing inmate rehabilitation.

4. **Purpose Code X (Exigent Procedures)--**Used when a QH query is executed during an emergency situation in which the health and safety of a specified group of individuals may be endangered. Following a QH query, a QR query may be used to review the individual's record. All requests for background checks for exigent purposes must be accompanied by fingerprints. This purpose code will only be used when directed by the Information Services Division Commander.