KANSAS CITY, KANSAS POLICE
GENERAL ORDER

ORDER NUMBER: **80.01**
ISSUED DATE: 11/04/2011
EFFECTIVE DATE: 11/04/2011
RESCINDS: 80.1 issued: 09/01/2006

SUBJECT: Criminal Records Information

REFERENCE: CALEA Ch.82

CROSS REFERENCE:

CONTENTS:

I. PURPOSE

II. DEFINITIONS AND AUTHORITY

III. CRIMINALHISTORYRECORD INFORMATION POLICY

IV. CRIMINAL HISTORY RECORD INFORMATION DISSEMINATION PROCEDURE

V. PUBLIC ACCESS TO IN-CAR VIDEO TAPES

VI. INTERSTATE IDENTIFICATION INDEX (III)

VII. NCIC RECORD VALIDATION

VIII. TRAINING

IX. VIOLATIONS

I. PURPOSE

A. To familiarize personnel with controls on the dissemination of criminal history record information (CHRI) to individuals, criminal justice, and other governmental agencies.

II. DEFINITIONS AND AUTHORITY

A. Computer Data: Any displayed information or printout information retrieved from a Police Department computer.

B. Records and Files: All official Police Department records, documents and files, other than those considered part of public record (public offense reports or traffic accident reports).

C. Conviction Data: Information or records that indicate an individual plead guilty to, or was convicted of, a criminal charge.

D. Non-Conviction Data: Information or records which indicate that a person was charged with a crime and one (1) or more of the following is listed as disposition of the charge.

1. The police elected not to refer the matter for prosecution.

2. The prosecutor elected not to pursue criminal prosecution.

3. Dismissed or acquitted of charges.

4. Any arrest record without a disposition in which one (1) year has elapsed from the date of arrest and no conviction has resulted and no active prosecution of the charge is pending.

E. NCIC: The National Crime Information Computer, which is maintained by the FBI. The FBI allows state and local law enforcement to enter information into NCIC, and access information in NCIC, such as stolen items, vehicles, and wanted persons.

F. Geographic Data: Information of any type that is processed through a geographic information system.

G. Statistical Data: Information requested to summarize a particular offense, area, category, crime rate or victim analysis.

H. Terminal Agency Coordinator (TAC): The Records and Technology Commander has the responsibility of coordinating NCIC use and ensuring NCIC compliance within the Department.

I. Full Access User: A terminal operator that both accesses information in NCIC and enters information into NCIC.

J. Less than Full Access User: An employee that runs inquiries on NCIC (including MDT's and Interstate Identification Index), but does not make entries into NCIC.

K. KCJIS – Kansas Criminal Justice Information System, which allows access to criminal history and other law enforcement information through the Kansas Bureau of Investigations.

III. CRIMINAL HISTORY RECORD INFORMATION POLICY

A. It is the policy of this Department that our criminal history record information is a record of arrests by Kansas City, Kansas Police. Since conviction data is not complete, all criminal history record information shall be treated as non-conviction data.

B. Dissemination of non-conviction data.

1. Dissemination is authorized to criminal justice agencies for the purposes of the administration of criminal justice and for justice agency employment.

2. Dissemination is allowed to individuals for any purpose authorized by statute, ordinance, executive order, or court rule, decision or order, as construed by appropriate state officials and executive officers of the Police Department.

3. Dissemination is authorized to individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to a specific agreement with a criminal justice agency. Such an agreement may only be authorized by the Chief of Police.

4. Non-conviction data will only be disseminated to members of the general public in accordance with section IV G of this order.

C. Dissemination of conviction data.

1. The Police Department does not enter or maintain conviction data. All requests for complete conviction data should be referred to the Kansas Bureau of Investigation, which is the official central repository for criminal history record information for the state of Kansas.

D. Dissemination to outside agencies.

1. Any field officer, Investigations Bureau member, Communications employee, or other Department employee who receives a request for criminal history information from anyone who is not a member of the Department shall refer that person to the Records and Technology Unit.

E. Logging of disseminations.

1. All disseminations of criminal history information from the Records and Technology Unit to anyone who is not a member of the Department shall be logged on the appropriate form. The logging form will include the necessary data on the subject whose record is requested, identification on the individual, the agency requesting the information, and the purpose of the request.

2. All personnel will use the appropriate logging mechanism when obtaining a copy of a criminal record or computer printout. Logging forms will be used when required by local, state, or federal regulations. Logging procedures are not necessary for department personnel when receiving information through the dispatcher or the mobile computer terminals.

F. Dissemination of computer data (non criminal history information)

1. Computer data information (such as vehicle registration or address checks) will only be released to law enforcement officers and then only after their identity has been verified. Persons other than law enforcement officers or persons not able to provide proof of their position as a law enforcement officer should be directed to the County Courthouse for public access information.

a. Identification of officers of this Department can be accomplished by asking for an item of personal information such as a serial number of other identifier and checking it against the officer's records.

b. Identification of officers of other departments can be accomplished by physically checking identification documents, if present, or by calling the person back through their police exchange, if the request is made by phone.

2. Social Security Numbers and Drivers License Numbers are not public records and cannot be released to the public.

IV. CRIMINAL HISTORY RECORD INFORMATION DISSEMINATION PROCEDURE

A. Requests for criminal history record information shall be handled only through the Records and Technology Unit.

B. Personnel in the Records and Technology Unit will comply with all applicable local, state, and federal laws and regulations when releasing any criminal history record information (CHRI).

C. Officer requests for wants or warrants on persons or property are still handled through the most convenient CHRI computer system.

D. Criminal history record information will only be disseminated to:

1. Members of this Police Department.

2. Authorized representatives or agents of any agency listed on the latest "CHRI valid users list."

3. Individuals requesting access to their own records upon showing proper identification, in accordance with IV G below.

4. Any person who submits an appropriate request and who is authorized to receive the particular CHRI by applicable local, state, and federal regulations.

5. Any exceptions authorized by the Commander of the Records and Technology Unit, the Services Bureau Director, or the Chief of Police.

E. Dissemination of Criminal History will only be done in the following manner:

1. No KCJIS data may be shared via electronic mail (e-mail) unless the shared users' email is on a secure network (LAN only connects criminal justice agencies and permits no modem or other communications connection) or is protected by a 128-bit encryption or higher.

2. Before dissemination of CHRI, including documents prepared by the employee that contain the substance of the CHRI, the employee must ensure that the other agency has a valid ORI and is authorized to receive CHRI. Dissemination of any CHRI outside of this agency must be logged and retained for two years. The log will include the name of the person, the agency's name and ORI, the date of dissemination, and the person to whom the information relates. Employee shall provide this log to administrative staff upon request.

3. Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHRI when an officer determines that there is an immediate need for the information to further an investigation or there is a situation affecting the safety of an officer or the general public.

4. CHRI may be transmitted via fax, but employee must telephone the receiving agency prior to transmission to verify the authenticity of the receiving agency and confirm the agency has a valid criminal justice ORI.

F. Access will be restricted to authorized persons in all areas in the Department where CHRI is available or maintained.

1. A logbook will be maintained for any person allowed into the secured area without an escort. Persons who are escorted need not be entered in the logbook.

2. All janitorial, maintenance, and other personnel employed or contracted by the Unified Government that may come into contact with criminal history record information in the Records and Technology Unit or on Police Department computers will be required to sign an "Awareness Statement for Personnel Not Authorized Access to Criminal History Record Information" form (attached). This is required by federal laws and criminal history regulations. Original forms will be retained in each employee's personnel jacket. A copy of each form will be retained by the Police Department.

G. The Records and Technology Commander will serve as the Police Department's Freedom of Information Officer. The Commander will familiarize themselves with the various provisions and exceptions outlined in the Kansas Open Records Act.

H. Persons have the right to review and challenge their criminal history record information that is retained by the Department. The Records and Technology Unit Commander is responsible for ensuring that all such disseminations of information are properly carried out and that they comport with NCIC regulations. This process will utilize forms provided by NCIC and/or the KBI.

1. Form 001, Request for Review of Individual Criminal History Record. This form is required for a person to access and review their criminal history information. The Records and Technology Commander or his designate will:

a. Fill out name, address, and telephone.

b. Record the date, initial the form, and state how the person was positively identified.

c. If the subject is accompanied, complete appropriate areas.

d. Allow the subject to review the record. The subject may make a handwritten copy or notations. A copy will NOT be provided to the subject.

e. Following review, have the subject complete, sign, and date the form.

f. Document this procedure by completing lower half of agency section.

g. Record the release in the dissemination log.

2. Form 002, Challenge of Criminal History Record. This form is used if the subject wishes to challenge an entry on their record.

a. The subject will be provided with a copy of the challenged portion of his or her record only.

b. The subject will be required to complete this form. A separate form will be used for each entry challenged, but they will be stapled together as one unit.

c. A copy of the completed form will be provided to the subject.

d. The Records and Technology Commander is responsible for responding to this form.

3. Form 003, Agency Response to Challenge. The Records and Technology Unit Commander will complete this form as the response to the challenge. A copy will be forwarded to the subject. If the challenge is denied, the Records and Technology Commander will also forward Form 004 in order to inform the subject that an appeal may be made.

4. Form 004, Appeals Request Form. This form will be included with the Agency Response to Challenge, if the Department is declining the challenge. It is the responsibility of the subject to complete this form and send it to the proper authority.

5. Form 005, Notification of Error in Criminal History Record Information. This form is used if the subject's challenge is determined to be valid, or if the Department is notified on appeal that there is an error in the subject's CHRI information that is maintained by the Department.

a. The Records and Technology Commander or his designate will determine whether any CHRI on the subject has been disseminated to other agencies within the prior year. This information should be available from the dissemination log or any notations accompanying the subject's record.

b. This form will be completed and forwarded to any agency to which CHRI was disseminated within the prior year.

V. PUBLIC ACCESS TO IN-CAR VIDEO TAPES

A. In-car videotapes are generally considered open records; it is not a requirement of the Open Records Act that the videotapes be reproduced. However, any videotape containing criminal investigation records, including vehicular homicide and any enforcement action more than a traffic violation, are not open records. Furthermore, incidents involving juvenile subjects (as suspects, victims, witnesses, CINC's etc.) are not open records.

B. Requests for any portion of a tape made by a citizen or an organization, other than the media (media requests will be handled in accordance with G.O. 50.1, media relations), will be referred to the Records and Technology Unit. All requests must be made in writing. The Records and Technology Unit Commander will contact the Division Commander, a Field Operations Bureau Commander, or Unit Commander who controls the requested tape. The Records and Technology Unit Commander may consult with the legal department to help make the determination if the requested material is an open record. Once the determination is made that the tape is open record the Bureau Commander will determine if the tape will be duplicated or viewed by the requesting organization. If the Bureau Commander deems necessary to duplicate the tape, the requesting person or organization for a standard fee can receive the duplicate version from the Records and Technology Unit Commander.

C. Original tapes will not be released from Police Department custody unless specifically approved by the Services Bureau Director or his designate.

VI. INTERSTATE IDENTIFICATION INDEX (III)

A. Interstate Identification Index inquiries are authorized for use in investigations and for screening applicants and employees for criminal justice agencies.

1. III will not be used for licensing purposes, except for armed security licenses. III will not be run for unarmed security permits.

2. III will not be used for routine traffic stops.

3. A subject will not be permitted to review his or her own III record.

B. III checks will be conducted periodically on Department employees who are full access and less than full access NCIC users. It is the responsibility of the Records and Technology Commander to ensure that these checks are completed and documented.

C. A logbook will be maintained for each III workstation, and the required entry will be made for all III requests.

1. Multiple III transactions should not be run on the same subject merely due to slow system responses. Even if the system is reacting slowly, once the transaction is sent, it will be processed by NCIC unless the computer ceases functioning. If multiple transactions on the same individual are needed, they will be appropriately logged.

2. If multiple III inquiries are conducted to get a "hit" on a subject using alternate information, this will be noted on the III log.

D. Operators who run III inquiries for officers will put the requesting officer's name in the attention (ATN) field followed by the operator's initials. The operator's name does not go in the ATN field. The officer requesting III information is responsible for the transaction, not the operator.

E. When a person entry is made into NCIC, (such as a missing person entry), a III and DMV inquiry must be made in order to complete the record. The III and DMV information will be filed with the report.

VII. NCIC RECORD VALIDATION

A. The FBI's NCIC Unit periodically prepares listings of records that are entered in the computer (stolen items, vehicles, missing persons, etc.). These lists are intended to verify that all information entered into NCIC by the Department is current. Certification by the Department of the listings means that:

1. The records contained on the validation listing have been reviewed by the Department;

2. The records which are no longer current have been removed from NCIC and all records remaining in the system are valid and active;

3. All records contain all available information; and

4. The information contained in each of the records is accurate.

B. The Terminal Agency Coordinator (TAC) will distribute portions of the list to those units that are responsible for confirming certain information. Verification lists are to be checked against Department records to ensure that the records are valid, active, accurate, and that they contain all necessary information. Discrepancies on the lists will be corrected in the NCIC system if possible. The lists must be returned to the TAC with all necessary remarks and corrections within 10 days.

VIII. TRAINING

A. Employees who have full access NCIC certification are required to re-certify every two years.

B. Less than full access personnel will undergo a period of training annually. The training may include such items as a review of CHRI policy, operating help for ASTRA, ALERT, NCIC, or a video training period prepared by Kansas Highway Patrol Certification personnel.

IX. VIOLATIONS

A. Once a violation has been discovered it is the supervisor's responsibility to immediately contact the Commander of the Technology Unit. The Technology Unit Commander shall report all violations to the CJIS System Officer (CSO) without delay. The report should be made immediately, but in no case shall the notification be withheld longer than the next business day.