502 KAR 30:050. Security of centralized criminal history record information.

RELATES TO: KRS 17.140
STATUTORY AUTHORITY: KRS 15A.060, 17.080, 17.140
NECESSITY, FUNCTION, AND CONFORMITY: KRS 17.080 authorizes the Secretary of Justice to institute rules and administrative regulations and direct proceedings and actions for administration of laws and functions that are invested in the Justice Cabinet. KRS 17.140 establishes, in the Justice Cabinet under the direction, control, and supervision of the Commissioner of the Department of State Police, a centralized criminal history record information system. KRS 17.140 defines a centralized criminal history record information system as the system including equipment, facilities, procedures, and agreements for the collection, processing, preservation, or dissemination of criminal history records maintained by the Justice Cabinet. This administrative regulation sets specific security standards to preserve the CHRI in an acceptable state.

Section 1. Procedures shall be implemented in the centralized criminal history record information system to insure that access to criminal history record information is restricted to authorized persons. The ability to access, modify, change, update, purge, or destroy such information shall be limited to authorized criminal justice personnel, or other authorized persons who provide operational support, such as programming or maintenance. Technologically advanced software and/or hardware designs shall be implemented to prevent unauthorized access to criminal history record information.

Section 2. Procedures shall be implemented in the centralized criminal history information system to determine what persons have authority to enter in areas where criminal history information is stored and implement access control measures to insure entry is limited to specific areas where authorization is valid. Further, access control measures shall be implemented to insure unauthorized persons are totally denied access to areas where criminal history record information is stored. Said access constraints shall include, but not be limited to, the system facilities, systems operating environments, data file contents, whether while in use or when stored in media library, and system documentation.

Section 3. Procedures shall be implemented in the centralized criminal history information system to insure that computer operations which support the criminal history record information data base, whether dedicated or shared, operate in accordance with procedures developed or approved by the Justice Cabinet, and further insure that:

(1) CHRI is stored by the computer in such a manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by unauthorized persons.

(2) Operational programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than designated terminals within the Records.

(3) The destruction, partial deletion, total deletion, or record correction is limited to designated terminals under the direct control of records.

(4) Operational programs are used to detect and store for the output of designated criminal justice agency employees, all unauthorized attempts to penetrate any criminal history record information system, program or file.

(5) The programs specified in subsections (2) and (4) of this section are known only to criminal justice agency employees responsible for criminal history record information system control or individuals in agencies pursuant to a specific written agreement with the Justice Cabinet to provide such programs and the operational program(s) are continuously kept under maximum security conditions.

(6) Procedures are instituted to assure that any individual or agency authorized direct access is responsible for:

(a) The physical security of criminal history record information under its control or in its custody; and

(b) The protections of such information from unauthorized access, disclosure or dissemination.

Section 4. Procedures shall be implemented in the centralized criminal history record information system to protect CHRI from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

Section 5. Emergency Plans Required. Written plans and instructions dealing with emergencies described in Section 4 of this administrative regulation shall be developed in manual form and cover all foreseeable incidents ranging from minor accidents to major disasters causing the destruction of computer facilities, entire data bases, and/or CHRI contained in manual files. Employees of the centralized criminal history record information system shall be trained in procedures and specifically assigned responsibilities in case of an emergency. Plans and instructions should be inclusive of, but not limited to, emergency shutdown and evacuation procedures, disaster recovery plan to restart critical system functions, procedures for back-up files for critical data such as fingerprint cards, and duplicate system designs. The Commissioner of the Department of State Police shall make available needed personnel to reinstitute the centralized criminal history record information system as soon as feasible after accident or disaster.

Section 6. The records commander shall institute procedures for the screening, supervising, and disciplining of agency personnel in order to minimize the risk of compromising internal security. A background investigation of all prospective employees for records shall be conducted. The scope of the background investigation shall be inclusive of, but not limited to:

(1) Verification of all items as listed on the employment application;

(2) Moral character;

(3) Financial history;

(4) Individual as well as spouse arrest history inclusive of juvenile files;

(5) Agency personnel records.

All records employees will agree to and sign nondisclosure statements and notice of security breach forms. The records commander shall so notify the Commissioner of the State Police as to any violation of security policy. A violation of said security policy shall include, but not be limited to, the intentional violation or wanton disregard of any or all security policies with regard to criminal history record information as set forth by section policy; the compromising of an employee's security by committing, facilitating, or being a party to a crime. Upon notification by the records commander of a security compromise, the commissioner shall take immediate appropriate administrative action. (11 Ky.R. 1717; eff. 6-4-85.)