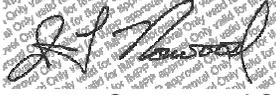


KANSAS DEPARTMENT OF CORRECTIONS

 Department of Corrections	INTERNAL MANAGEMENT POLICY AND PROCEDURE	SECTION NUMBER 05-172D	PAGE NUMBER 1 of 4
		INFORMATION TECHNOLOGY AND RECORDS: KCJIS Security Policy	
Approved By:  Secretary of Corrections		Original Date Issued: 06-16-16	
		Replaces Version Issued: N/A	
		CURRENT VERSION EFFECTIVE: 06-16-16	

APPLICABILITY:	_ ADULT Operations Only	_ JUVENILE Operations Only	<input checked="" type="checkbox"/> DEPARTMENT-WIDE
-----------------------	-------------------------	----------------------------	---

POLICY STATEMENT

The Kansas Department of Corrections (KDOC) recognizes and accepts the KCJIS Security Policy, CJIS Security Policy included, as the minimum set of security requirements for access to systems and information of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division in order to protect and safeguard Criminal Justice Information (CJI). All other policy or procedures by any KDOC entity shall complement the KCJIS Security Policy, however, the KCJIS Security Policy shall always be the minimum standard and local policy may augment or increase the standards, but shall not detract from the KCJIS Policy standards.

All KDOC contractors using any KDOC network(s) shall comply with this policy specifically the KCJIS Security Policy.

All entities having access to KDOC data online shall comply with background requirements and IT security awareness requirements of the KCJIS Security Policy.

All KCJIS equipment use, including any mobile device authorized for direct KCJIS access, tokens and systems, is limited to the primary mission of the Kansas Department of Corrections.

DEFINITIONS

Agency: For purposes of this IMPP, this is any KDOC entity that submits or receives information, by any means, to/from the FBI, CJIS system or services and/or to/from the KCJIS system or services.

Authorized Users: For purposes of this IMPP, any full-time, part-time, or temporary, volunteer, contract employee or anyone else working for the local entity who is approved to personally use information systems to directly request CJI or who has CJI provided to them.

Data/Information: For purposes of this IMPP, both terms refer to Criminal Justice Information (CJI).

KBI: Kansas Bureau of Investigation is the Kansas agency responsible for running the KCJIS network, activating tokens, and providing access to repository applications and data.

KCJIS Equipment: To include tokens, desktops, laptops, or any mobile device authorized for direct KCJIS access.

KHP: Kansas Highway Patrol is the Kansas agency designated by CJIS as responsible for establishing and administering the information technology security program throughout the user community.

LASO: Local Agency Security Officer is a position required by KCJIS to ensure compliance with KCJIS security requirements.

TAC: Terminal Agency Coordinator is a position required by KCJIS to serve as the point of contact at the local agency for matters relating to KCJIS information access.

PROCEDURES

I. Roles and Responsibilities

- A. Each KDOC entity with direct KCJIS access shall appoint a TAC, at least one Alternative TAC, and a LASO to carry out the KCJIS administration and responsibilities required by the KCJIS Security Policy, the Kansas Highway Patrol, and the Kansas Bureau of Investigation.
 - 1. The TAC and the Alt TAC positions shall be filled by two separate individuals.
 - 2. The TAC, the Alt TAC, and the LASO shall attend training and maintain certifications as required by the KHP.
 - 3. The TAC, the Alt TAC, and the LASO shall be aware of and shall conform to all deadlines and requirements of the KHP.
 - 4. TAC/Alt TAC Responsibilities
 - a. The TAC/Alt TAC shall perform all responsibilities as required by the KCJIS Security Policy.
 - b. The TAC and Alt TAC shall refer to the KHP's TAC Manual for guidance and requirements in performing their KCJIS responsibilities.
 - 5. LASO Responsibilities
 - a. The LASO shall perform all responsibilities as required by the KCJIS Security Policy
- B. Authorized Users
 - 1. Employees of the local entity who are approved to personally use information systems to directly request CJI or who have CJI provided.
 - a. Authorized users shall be backgrounded in accordance with KCJIS policy using the TAC Manual for guidance.
 - b. Authorized users are prohibited from running their own background check or seeing the results of their own background check.
 - c. Authorized users are prohibited from running the background checks of family members or seeing the results of background checks on family members.
 - d. Authorized users with direct KCJIS access shall be alert for the presence of others and shall ensure that non-authorized users are not able to view the computer screen when CJI is displayed.
 - 2. Authorized users with printed CJI shall ensure the security and protection of the printed CJI until destroyed in a manner prescribed by KCJIS Security Policy.

C. Other Users

1. Users with authorized access to stored CJJ (e.g., FBI #, KBI #, imaged III, etc.) shall not open email from a mobile device (e.g., cell phone, tablet, etc.) that is not protected with encryption.
2. Employees who violate any portion of this policy or the KCJIS Security Policy are subject to disciplinary procedures as outlined in KDOC IMPP 02-120, Employee Disciplinary Procedures and Informal/Formal Actions.
 - a. Failure to comply with all provisions of this policy may be grounds for discipline, up to and including dismissal.

II. **Administrative Security**

A. Dissemination of CJJ

1. Dissemination of CJJ is authorized only to other criminal justice agencies once a need to know has been verified.
2. When dissemination of CJJ, especially CHRI, is made to a criminal justice agency, that dissemination shall be recorded in a secondary dissemination log maintained in the offender record for no less than 3 years.

B. Training of all persons having access to Criminal History information

1. All personnel shall be trained within 6 months of selection or assignment on privacy and security issues regarding the use of CJJ.

C. Lost or Stolen CJIS Equipment

1. The local TAC shall be notified within 1 work day upon determination that any KCJIS equipment is lost or stolen.
2. The local TAC shall notify the KBI Help Desk immediately of the lost or stolen equipment.

NOTE: The policy and procedures set forth herein are intended to establish directives and guidelines for staff and offenders and those entities that are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or offenders, or an independent duty owed by the Department of Corrections to employees, offenders, or third parties. Similarly, those references to the standards of various accrediting entities as may be contained within this document are included solely to manifest the commonality of purpose and direction as shared by the content of the document and the content of the referenced standards. Any such references within this document neither imply accredited status by a Departmental facility or organizational unit, nor indicate compliance with the standards so cited. The policy and procedures contained within this document are intended to be compliant with all applicable statutes and/or regulatory requirements of the Federal Government and the state of Kansas. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

REPORTS REQUIRED

None.

REFERENCES

Criminal Justice Information Systems (CJIS) Policy
Kansas Criminal Justice Information Systems (KCJIS) Policies and Procedures

ATTACHMENTS

None.