

New Agency Information And Request Forms For KCJIS Access

Welcome to the Kansas Criminal Justice Information System.

The Kansas Criminal Justice Information System (known simply as KCJIS) is a system of connected data sources within a secure environment supporting the electronic exchange of information for local, state and national criminal justice interests.

This packet is designed to assist your agency in obtaining **access** to KCJIS **via the Kansas Central Message Switch**, to include access to Nlets and FBI CJIS systems such as NCIC and III.

Here are a few of the things to be aware of when considering your agency's commitment to KCJIS.

Criminal Justice Information (CJI) is the term used to refer to all of the FBI CJIS and KCJIS provided data necessary for law enforcement and civil agencies to perform their missions. Criminal History Record Information (CHRI) is a subset of CJI. Use and dissemination of CJI and CHRI are outlined in Title 28, Part 20, Code of Federal Regulations (CFR), the NCIC Operating Manual, FBI CJIS Security Policy, and KCJIS Policies and Procedures. Kansas CHRI is subject to K.S.A. 22-4701 et. seq.

These referenced policies, regulations, and statutes are available for review via the [KHP CJIS Launch Pad](#). All agencies with access to CJI are responsible for the protection of CJI by adherence to these policies.

Personnel Requirements

Personnel Screening and Training

Personnel with unescorted/unmonitored access to: CJI in any media format, areas where CJI is used, or computers and network infrastructure used to access CJI must be authorized for access by:

1. Undergoing an initial fingerprint-based record check for criminal history, followed by annual name-based rechecks as described in KCJIS Policies and Procedure 5.12.
 - a. Some disqualifiers and other requirements are included in this policy area.
2. Complete Security Awareness and other training requirements according to their level of access to CJI as outlined in KCJIS Policies and Procedure 5.2. For more information go to <https://cjisaudit.khp.ks.gov/launchpad/training/training.cgi>

Terminal Agency Coordinator (TAC)

Each agency with their own computer access to KCJIS must designate at least one individual as their Terminal Agency Coordinator (TAC). Two alternates may also be designated.

The TAC is responsible for:

- Overseeing the administrative aspects relating to the use of their agency's access to KCJIS such as adding or removing active users and assigning RSA tokens for each user.
- Ensuring the information entered into KCJIS and NCIC is accurate and complete and that CJI obtained from KCJIS and NCIC is used and disseminated according to policies.
- TAC training administered by the Kansas Highway Patrol CJIS Unit is required.

New Agency Information And Request Forms For KCJIS Access

Local Agency Security Officer (LASO)

Each Agency with access to CJI must also have someone designated as the Local Agency Security Officer (LASO). It is acceptable, and even common, for the TAC and LASO roles to be assigned to the same person. Alternates can be identified within your agency, however only one LASO can be designated in the current KCJIS system.

Each LASO shall:

- Identify who is using the approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
- Identify and document how agency equipment is connected to KCJIS.
- Ensure that personnel security screening policies are being followed.
- Ensure approved and appropriate security measures are in place and working.
- Support policy compliance and ensure CSA ISO is promptly informed of security incidents.
- Be responsible for securing security awareness training and associated record keeping.

Get an Originating Agency Identifier (ORI)

Access to KCJIS and FBI CJIS systems requires an Originating Agency Identifier (ORI).

Generally, to qualify for an NCIC ORI agencies must be a criminal justice agency as specified in Title 28 Code of Federal Regulations Part 20 Subpart A §20.3:

"(g) Criminal justice agency means: (1) Courts; and (2) a governmental agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice. State and Federal Inspector General Offices are included."

("allocates a substantial part of its annual budget" has been interpreted to mean more than 50 percent by the originator of the Regulations).

"(a) Administration of criminal justice means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information."

If you believe your agency qualifies for an ORI send your request on agency letterhead along with a copy of the ordinance, statute, and/or other legislative action supporting your request to:

Kansas Highway Patrol CJIS Unit
Attention: NCIC ORI Coordinator
122 SW 7th Street
Topeka, KS 66603
Fax: 785-296-0958.

You may email digital images of the information to khpcjis@khp.ks.gov.

The KHP will forward your request to the FBI CJIS access group who determines eligibility and assigns NCIC ORIs.

New Agency Information And Request Forms For KCJIS Access

Determine how your agency will obtain CJI from KCJIS.

You may 1) Get your own device access (see [System Requirements](#) below) and/or 2) arrange for current terminal agencies to access KCJIS on your agency's behalf.

With either option, your agency needs to consider how messages from KCJIS meant for your agency will be received and handled when your agency does not have a working KCJIS computer.

For instance: Your agency may have record entries - made by your own staff or on your agency's behalf - in NCIC. Those entries may result in another agency's query "hitting" on your agency's entry. When a hit occurs, a hit confirmation request is sent back through the system intended for the agency of the record (you) to confirm the validity of the information. Arrangements need to be made so other agencies responding to hit confirmations on your behalf can verify the current status of your entries.

Complete at least one [KCJIS 114 Inter-Agency ORI User and Holder of Record Agreement](#) to setup *another agency as a Serving Agency* in order to make entries or query CJIS systems on your User Agency's behalf.

- A 24 hour process can be arranged to contact your agency to physically check records on file and confirm them within the required response time limit.

Or,

- Complete Part III of the KCJIS 114 Inter-Agency ORI Use and Holder of Record Agreement if your agency will be providing the Serving Agency with a set of records for all entries made by or on behalf of your agency. Your agency will need to keep this set of records current. This can be through a shared Electronic Record Management System (E-RMS).

System Requirements (Internet, RSA Tokens, Hardware, Software, System Security)

1. Internet connection:

Internet service is required for access. Any commercial grade Internet Service Provider available in your area will work. Or, if none are available, the State of Kansas' Office of Information Technology Service (OITS) may be available (KHP can arrange contact with OITS for latest rates). A commercial internet connection can be shared with other governmental agencies so long as *controls are in place to ensure no unencrypted CJI is accessible by unauthorized personnel, to include separation from non-criminal justice by a firewall*.

New Agency Information And Request Forms For KCJIS Access

2. RSA SecureID Tokens are required for each user ID accessing KCJIS systems. Procurement of tokens is the agency's responsibility. Orders for tokens can be made on Agency letterhead to OPTIV security and you will need to advise how you will be paying for them. OPTIV ships the tokens to the KBI who configures them for KCJIS access and then forwards them to your agency.

OPTIV's contact information (subject to change) is:

OPTIV Security
6130 Sprint Parkway, suite 400
Overland Park, KS 66211
Phone (sales) 888-732-9406
FAX 816-421- 6677
tokens@optiv.com

3. Hardware and Software for KCJIS provided applications and services
KCJIS systems are designed to work with the following:

Client operating systems and hardware:

- Microsoft® Windows 7 Manufacturer extended Support through January 14, 2020
- Microsoft® Windows 10 Manufacturer extended Support through October 14, 2025

Processor: Intel® Pentium®, Celeron®, Core® processor or equivalent (2.00 GHz or faster)

Memory: 2 GB or more system RAM

Hard Drive: 40 GB or more, with 1 GB or more free space

Java Runtime Environment (for OpenFox):

The latest supported version is available from the KCJIS OpenFox Desktop Web Portal
<http://cpi.kcjis.state.ks.us:8080/KAN/>

Server Operating Systems and hardware (dependent on software vendor compatibility):

- Microsoft® Windows Server 2008 Manufacturer Extended Support through 1/14/2020
- Microsoft® Windows Server 2008 R2 Manufacturer Extended Support through 1/14/2020
- Microsoft® Windows Server 2012 Manufacturer Extended Support through 1/10/2023

Processor: Intel® Xeon® or equivalent (2.00 GHz or faster)

Memory: 2GB or more system RAM

Hard Drive: 40 GB or more, with 1 GB or more free space

Web Browser: Microsoft® Internet Explorer (IE) version 11

Contact your KHP technical auditor or the KBI helpdesk if additional specifications and support options are needed.

New Agency Information And Request Forms For KCJIS Access

4. Security Requirements

Encryption:

CJI transmitted outside physically secure locations must be encrypted to Federal Information Processing Standard (FIPS) 140-2 as certified by the National Institute of Standards and Technology (NIST).

- A Virtual Private Network (VPN) is required to access most KCJIS information systems:
 - Check Point SecuRemote client VPN is available for download from the secure KCJIS portal once you have active user ids and tokens.
 - Firewall to Firewall (aka Site to Site) VPN details are available from the KBI Helpdesk or KCJIS technical auditor.
- NIST certified encryption is also required between your local secure network(s) and remote devices outside secure criminal justice networks.

CJI stored electronically outside a physically secure location must be encrypted using FIPS 197 certified (AES 256) products or FIPS 140-2 certified modules.

Additional security requirements for all devices accessing KCJIS:

- Protection against malware (viruses), spam and spyware. This can be a single security suite or separate applications.
- Intrusion Detection installed for all information systems* processing CJI.
- A firewall that users cannot disable must be used to keep criminal justice and non-criminal justice networks separated. Host based firewalls can be used on each device.

Virtual Local Area Networks (VLANs) are acceptable when criminal justice systems are maintained on their own VLANs and the requisite segregation is retained through to a firewall.

- * Devices used to access KCJIS wirelessly are considered their own "information system" and must have the same equivalent functionality of security and protections as your wired devices.
 - A Mobile Device Management (MDM) system with centralized administration must be implemented for devices with limited feature operating systems (iPhones, Android, etc.).

New Agency Information And Request Forms For KCJIS Access

Complete and submit appropriate agreements and forms.

The agency responsible for each of these forms is identified in parenthesis below. You may submit all forms in this packet to the KHP CJIS Unit who will forward necessary forms to the KBI.

- a. [Memorandum of Understanding for Kansas Criminal Justice Agencies Accessing KCJIS Portal](#) must be reviewed, signed by agency head and TAC. (KBI)
- b. Submit a [KCJIS 188 KCJIS Agency Contact Form](#) in its entirety. (KHP)
Refer to Agency Administrative Roles on page 1.
- c. Submit a signed [KCJIS 115 Agency Connectivity Agreement](#) (KHP).
- d. Submit a [KCJIS 118 Device Connection Request form](#) entering the quantities of each type of device you plan to deploy within 30 days. (KHP)
 - Your TAC(s) will need at least 1 computer with a VPN connection capable of accessing the KACIS web page.
 - To access NCIC, III and other federal systems the TAC(s) will also need a computer with KCJIS supplied OpenFox with the "configurator" module.
 - You may request additional computers with VPN connectivity with only the OpenFox messenger module as needed for efficient use and access by general KCJIS users.
 - You may also request access to KCJIS using server based software of your own or another agency if it has been tested by the KBI and verified compatible with KCJIS.
- e. Submit the [KCJIS 105 Network Security Questionnaire](#). (KHP)
 - A network diagram must accompany the KCJIS 105 showing locations of wired devices as they relate to the firewalls, separation from non-criminal justice systems, etc.
- f. Submit a [KCJIS 232 Encryption Questionnaire](#) to confirm ALL options that will be used by your agency to transmit or store CJJ outside your physically secure location. (KHP)
- g. Complete a [KCJIS 239 Mobiles Data Device Questionnaire](#) if applicable. (KHP)

Once approved

- Your KHP CJIS Unit technical auditor will notify all stakeholders by email.
- Contact the KBI Helpdesk (785-296-8245) to arrange implementation within 30 days.
- The KHP CJIS Unit will ensure your agency access to CJIS Audit and NexTEST from the KHP CJIS Launch Pad for access to KCJIS information, audit and training materials.

Kansas Criminal Justice Information System

Inter- Agency ORI Use and Holder of Record Agreement

This agreement provides for _____, ORI # _____,
hereafter referred to as the *Serving Agency*,

to access KCJIS on the behalf of _____, ORI # _____,
hereafter referred to as the *User Agency*, with respect to the provisions as indicated below.

(Check all that apply):

PART I KCJIS Systems Access

- KACIS Agency Administration** - The Serving Agency may add, modify and remove KCJIS users for the User Agency.
- E-Disposition entry** - The Serving Agency may enter, modify, and otherwise transact disposition reporting as required by law on behalf of User Agency if User Agency is a Court or Prosecutor.
- KSORT** - The Serving Agency may enter, modify, and otherwise transact on behalf of the Sheriff regarding KSORT.
- Prelog/Case Inquiry** – The Serving Agency may view and download User Agency case information.

PART II Central Message Switch Access

- The Serving Agency will only query NCIC, III, KCJIS and other criminal justice records on behalf of the User Agency.
- The Serving Agency may query, make entries, modifications, cancellations and clear records contained in NCIC and KCJIS files. The Serving Agency shall use the User Agency's ORI unless a Holder of Record Agreement (Part III of this agreement) exists.
 - The User Agency has no other access to KCJIS and requests the SERVING Agency act as their PRIMARY access resource.
 - The User Agency has their own or other access to KCJIS, and request the Serving Agency act as a SECONDARY access resource ("Trouble Node").
- The Serving Agency agrees to immediately act on messages addressed to the User Agency according to previously agreed on procedures. These messages may include but are not limited to:
 - Emergency and priority messages
 - Hit confirmations as required by the FBI and KCJIS policies
 - Check Here and Complete Part III if Serving Agency will act as Holder of Record
 - Messages received on behalf of the User Agency that indicate communication failures ("trouble node" notices) thus alerting the User Agency to message delivery problems

Kansas Criminal Justice Information System

Inter- Agency ORI Use and Holder of Record Agreement

PART III Holder of Records

The Serving Agency shall act as a "Holder of Records" for the User Agency.

The User Agency shall furnish the Serving Agency all available documentation pertinent to any records entered into Criminal Justice Systems on behalf of the User Agency to ensure compliance with FBI CJIS and KCJIS policies, rules and regulations delineating the responsibilities of the agency entering any such transactions. This documentation shall be in the form of:

Access to a shared electronic Records Management System that is maintained by_____.

And/or (check all that apply)

Hard Copy printouts delivered to the Serving Agency with updated records provided to the Serving Agency within _____ hours of new information becoming available to the User Agency.

The Serving Agency shall perform all records validations procedures as required by FBI CJIS, NCIC, and KCJIS policies, rules and regulations.

or

The User Agency shall perform all records validations procedures as required by FBI CJIS, NCIC, and KCJIS policies, rules and regulations.

PART IV Personnel Screening and Training

For all User Agency personnel authorized to access Criminal Justice information (CJI), **the SERVING Agency agrees to** provide the following as required by FBI CJIS and KCJIS policies:

Record checks (Fingerprint, name-based records check and annual name-based records check)

Security Awareness training (within the first 6 months of hire and every 2 years thereafter).

NCIC Certification Training (within the first 6 months of hire and every 2 years thereafter)

For all User Agency personnel authorized to access Criminal Justice information (CJI), **the User Agency agrees to** provide to the Serving Agency evidence of completion of the following as required by FBI CJIS and KCJIS policies:

Record checks (Fingerprint, name-based records check and annual name-based records check)

Security Awareness training (within the first 6 months of hire and every 2 years thereafter).

NCIC Certification Training (within the first 6 months of hire and every 2 years thereafter)

Kansas Criminal Justice Information System
Inter- Agency ORI Use and
Holder of Record Agreement

PART V Miscellaneous

Both agencies agree to abide by all rules, policies and procedures of FBI CJIS, NCIC, NLETS, and KCJIS, and any amendments thereto.

This is a formal expression of the intent of both agencies and is effective when signed.

The User Agency indemnifies and absolves the Serving Agency, including its officials and employees, of all liability for any claims, demands, actions, costs, expense, or damage resulting from any breach of this agreement by the User Agency, or on any use or misuse made of information or services furnished to the User Agency by the Serving Agency.

This agreement is being executed by officials of the agencies in their representative capacities. Accordingly, this agreement will remain in effect after the officials vacate their positions and/or until it is affirmatively amended or rescinded in writing (it may be amended after written concurrence of both agencies).

The Serving Agency may immediately suspend this agreement when either the security or dissemination requirements adopted by FBI CJIS, NCIC, NLETS, or KCJIS are violated. In such instances, the Serving Agency may reinstate this agreement upon satisfactory assurances that such violation has been corrected.

Upon determination by KCJIS administrators (KHP or KBI) that a security incident or policy violation has occurred by either agency, this agreement shall be suspended until KCJIS authorities have been provided satisfactory assurances that such incident or violation has been properly addressed and corrected.

This agreement does not confer, grant, or authorize any additional rights, privileges, or obligations to any third party.

Signature for the Serving Agency Date

Printed Name

Title

Signature for the User Agency Date

Printed Name

Title

**MEMORANDUM OF UNDERSTANDING
FOR KANSAS CRIMINAL JUSTICE AGENCIES
ACCESSING KCJIS PORTAL**

This Memorandum of Understanding (MOU) is for use with all Kansas criminal justice agencies, or governmental non-criminal justice agencies under the management control of a criminal justice agency, which require access to intrastate criminal justice information systems (hereinafter referred to as the User). This access will be provided by and administered by the Kansas Bureau of Investigation (KBI) and the Kansas Highway Patrol (KHP) through the Kansas Criminal Justice Information System (KCJIS).

The KBI and KHP will facilitate User's requests to participate in the information services provided on KCJIS, provided the User agrees to abide by all applicable laws, administrative rules, regulations, policies and/or procedures related to these systems.

KCJIS provides access and participates in various state criminal justice databases and files, which include but are not limited to: Kansas adult and juvenile criminal history record information (CHRI) maintained by the KBI, information provided and maintained by Kansas Department of Corrections (DOC), Kansas Juvenile Justice Authority information (JJA), and Kansas Office of Judicial Administration (OJA); and KCJIS "hot files" such as the Kansas warrants, registered offenders, missing persons, and the "Be On the Lookout" file (BOLO).

The KBI is responsible for establishing and maintaining KCJIS, including the network and related security issues, technical help desk, hardware, software, and interfaces.

The KHP is responsible for approving access to KCJIS, as well as auditing those agencies to ensure compliance to applicable laws, administrative rules, regulations, and KCJIS policies and procedures. The KHP is responsible for training on KCJIS policies and procedures. Training on the proper use and dissemination of other information provided through KCJIS shall remain the responsibility of the agency governing the data.

Final approval of all policies and procedures will rest with the Kansas Criminal Justice Coordinating Council (KCJCC).

User agrees to adhere to the following to ensure continuation of access:

ADMINISTRATIVE POLICIES

1. Information obtained from KCJIS can only be used for criminal justice purposes in compliance with all applicable laws administrative rules, regulations, policies, and procedures related to these systems. It is the responsibility of the User to ensure access to KCJIS is used for authorized criminal justice purposes only; provide training on proper access, usage and dissemination of data obtained through KCJIS; and document, implement, and enforce agency policies, procedures, sanctions and discipline procedures for misuse of data obtained through KCJIS. Agencies that interface between KCJIS and other criminal justice agencies must abide by all provisions of this agreement. Agencies that access KCJIS by interfacing through other agencies must, likewise, abide by all provisions of this agreement.
 - a) **COMPLIANCE:** Operate the workstation or access device in strict compliance with all applicable KCJIS policies including, but not limited to, policies and procedures relating to:
 - **TIMELINESS:** Use of KCJIS hot files is optional, however, if records are maintained in KCJIS, the records should also be entered, modified, cleared or canceled promptly to ensure system effectiveness.
 - **HOT FILE ENTRIES:** User agencies that maintain a 24-hour, seven day a week operation, will be allowed to make entries into the KCJIS hot files. For non-24 hour operations, a Criminal Justice ORI User Authorization Agreement must be executed with a 24X7X365 User agency in order to handle hit confirmations and unsolicited messages.
 - **QUALITY ASSURANCE:** Appropriate and reasonable quality assurance procedures must be in place to ensure all entries/records in KCJIS hot files are complete, accurate and valid.
 - **VALIDATION:** The User must validate all records that the agency has entered into applicable KCJIS hot files for accuracy and retention. To be in compliance, the User agency must ensure each record is modified to confirm the hot file record is still active and information contained is valid.
 - **HIT CONFIRMATION:** User must comply with KCJIS policies by responding to hit confirmations in a timely manner (within 10 minutes or one-hour, depending upon priority.)
 - **DISSEMINATION:** Information obtained from KCJIS can only be used for criminal justice purposes and only for the purpose for which the request was made. The data maintained in KCJIS is documented criminal justice information, and this information must be protected to ensure correct, legal, and efficient

dissemination and use. The individual receiving a request for KCJIS information must ensure that the person requesting the information is authorized to receive the data. The commercial dissemination of information obtained through KCJIS is prohibited. Copies of CHRI data obtained through KCJIS must be afforded security to prevent any unauthorized access to or use of the data. CHRI records must be maintained in a secure records environment. Such storage of records will be maintained for extended periods only when CHRI records are key elements for the integrity/utility of the case files/criminal records where they are retained. When retention of the CHRI record is no longer required, disposal will be accomplished in a secure manner so as to thoroughly destroy all elements of the records and preclude unauthorized viewing, access, or use.

- i) Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of criminal history record information (CHRI) obtained through KCJIS, 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.
 - ii) A facsimile device may be used to transmit hard copy criminal history records provided both agencies involved have valid ORIs, and are authorized to receive criminal history. The transmission of facsimile information must meet the same security considerations as dial-up access including identification and authentication; therefore, telephone notification prior to the transmission shall be initiated to verify the authenticity of the receiving agency.
 - iii) No information obtained through KCJIS can be copied and transmitted via unsecured electronic mail (e-mail).
- **LIABILITY:** User understands that the KBI and KHP, its officers and employees shall not be liable in any claim, demand, action, suit, or proceeding, including but not limited to, any suit in law or in equity, for damages by reason of, or arising out of, any false arrest or imprisonment or for any loss, cost, expense or damages resulting from or arising out of the acts, omissions, or detrimental reliance of the personnel of the User in entering, removing, or relying upon information in the KCJIS.
 - **CRIMINAL HISTORY RECORDS:** Kansas CHRI is maintained by the KBI. These records shall be used solely for such purposes as provided by Kansas statutes. These include but are not limited to: Kansas Statutes Annotated (KSA) 22-4701 et seq., KSA 38-1608, KSA 38-1618, and Kansas Administrative Regulations (KAR) 10-12-1 et seq., and KAR 10-19-1 et seq. User shall ensure that access to all CHRI furnished, to include documents prepared by the receiver that contain the substance of the CHRI, is restricted to persons directly involved in the professional use for which the CHRI is obtained, and is disseminated only in strict accordance as outlined in this MOU.

2. Unless specifically exempted, each person accessing KCJIS must have a permanently assigned KCJIS access token. Tokens cannot be shared among users.
3. Each person accessing KCJIS shall not leave their workstation or access device logged onto the network while away from the equipment. This may be accomplished by logging off the network or locking the keyboard/access where the employee's password is required.
4. KCJIS will maintain an electronic log of criminal justice information obtained through KCJIS for a minimum of two years. The User must maintain a record of any further (indirect) dissemination of KCJIS information to other authorized criminal justice agencies, including the name of person, the agency's name and ORI, the date of dissemination, and the person to whom the information relates for a period of two years. This log must be made available upon request by authorized KCJIS staff.
5. All KCJIS information shall be securely stored and/or disposed of to prevent unauthorized personnel. This includes fixed storage media, e.g. hard disks, RAM disks, removable media back-up devices, as well as printed documents. Disposal procedures shall include a method sufficient to preclude recognition or reconstruction of the information.
6. Each agency administrator must designate at least one, but up to three, employee(s) to be the terminal agency contact (TAC) for KCJIS related matters. TACs responsibilities include:
 - Coordinate agency's terminal requests, when appropriate.
 - Assign user portal access rights and privileges.
 - Assign and administer agency KCJIS tokens.
 - Maintain agency site/user information in KCJIS.
 - Document training to agency users on proper access, usage, and dissemination of KCJIS data.
 - Act as point of contact regarding compliance issues, security matters and audits conducted by state. Responsible for distributing publications and training materials to affected agency personnel.
 - Responsible for validating agency's records maintained in state hot files.
 - Attend KCJIS-related training.
 - Install or coordinate installation of KCJIS-related software. The TAC may notify the KBI Help Desk, in writing, the name and telephone number of an information technology staff person point of contact (IT POC) who may act on behalf of the agency's TAC and obtain sensitive information in order to download certificates of authority.

ACKNOWLEDGEMENT: User hereby acknowledges and agrees to the provisions and responsibilities as set out in this MOU. User further acknowledges that failure to comply with any of these provisions and/or responsibilities may subject its agency to various sanctions; these sanctions may include complete termination of KCJIS access.

TERMS OF AGREEMENT: This agreement will remain in force until it is determined by the KBI that a new agreement is required. The signed agreement will remain on file at the KBI. The User agency should initiate the execution of a new agreement when a change of agency administrator or TAC occurs.

DATE: _____

AGENCY NAME: _____

TELEPHONE NUMBER: _____

AGENCY HEAD: _____
(Please Print)

(Signature)

PRIMARY TAC: _____
(Please Print)

(Signature)

SECOND TAC: _____
(Please Print)

(Signature)

THIRD TAC: _____
(Please Print)

(Signature)

Return to: KBI Communications Unit
1620 SW Tyler
Topeka, KS 66612-1837
Fax: 785-296-7154

KCJIS AGENCY CONTACT FORM

Complete each section of the form that applies to your agency, by including ALL current TAC, LASO and Agency Head assignment information each time you submit this form. This information should reflect the information listed in KACIS and nexTEST.

AGENCY NAME: _____ ORI: _____

TAC #1	Name: _____ User ID: _____ Phone: _____ Fax : _____ E-mail: _____ Remove: _____ User ID: _____
TAC #2	Name: _____ User ID: _____ Phone: _____ Fax : _____ E-mail: _____ Remove: _____ User ID: _____
TAC #3	Name: _____ User ID: _____ Phone: _____ Fax : _____ E-mail: _____ Remove: _____ User ID: _____
AGENCY HEAD	Name: _____ User ID: _____ Title: _____ Phone: _____ Fax : _____ E-mail: _____ Remove: _____ User ID: _____
LASO	Name: _____ User ID: _____ Phone: _____ Fax : _____ E-mail: _____ Remove: _____ User ID: _____

Note: This form must be signed by an authorized person (either an already-existing TAC, or an already-existing agency head)

Authorizing Signature: _____ Date: _____

KANSAS CRIMINAL JUSTICE INFORMATION SERVICES
AGENCY CONNECTIVITY AGREEMENT

Agency Name: _____ ORI: _____

The Kansas Criminal Justice Information System (KCJIS) provides identification and information services to the criminal justice communities in Kansas. Under certain circumstances allowed by federal or state laws, the noncriminal justice community may also be granted access. KCJIS services are primarily maintained by the Kansas Bureau of Investigation and are administered and managed between the Kansas Bureau of Investigation and the Kansas Highway Patrol. The Kansas Highway Patrol is the designated FBI CJIS Systems Agency (CSA) for Kansas with oversight over access to FBI CJIS Systems. The KCJIS Committee established by K.S.A. 74-5701 *et seq.* establishes, maintains, and upgrades the KCJIS and adopts rules and regulations as needed.

The Kansas CJIS Systems Agency is required to provide access to certain FBI CJIS services and does so by way of the KCJIS. The KCJIS also provides access to specific state databases. The following services are provided to connecting agencies and users, as applicable:

1. Access to FBI CJIS Systems that include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS).
2. Access to various state of Kansas databases and files, which include but are not limited to: criminal justice information in Kansas Offender Registration files, Kansas adult and juvenile criminal history record information (CHRI), information provided and maintained by Kansas Department of Corrections (DOC), and Kansas Office of Judicial Administration (OJA) and non-criminal justice information in systems maintained by non-criminal justice agencies such as Kansas Department of Revenue (KDOR) and Kansas Department of Transportation (KDOT).
3. Operational, technical, and investigative assistance.
4. System automation, when feasible, to ensure policy compliance.
5. Information System audit and review including logging of certain activities occurring through KCJIS as required by policies.
6. Information as needed on all aspects of FBI CJIS and KCJIS Systems and related programs by means of the Internet based information websites; KCJIS web portal, KCJIS newsletters, information letters, and other relevant documents and resources.
7. Training materials and assistance to each Terminal Agency Coordinator (TAC), Local Agency Security Officer (LASO), and other appropriate personnel.
8. Procedural audits of agencies to ensure compliance with applicable policies.

KANSAS CRIMINAL JUSTICE INFORMATION SERVICES
AGENCY CONNECTIVITY AGREEMENT

The connecting agency (hereafter referred to as “the Agency”) agrees to adhere to all policies, regulations, and laws referenced in this agreement that include, but are not limited to:

1. **Quality Assurance** – The Agency will document appropriate procedures to ensure that only complete, accurate and valid information is maintained in State and Federal Criminal Justice Information systems, and that information is readily available to respond to requests for information by authorized parties, such as hit confirmations.
2. **Training** – The Agency is responsible for training requirements, including compliance with operator training mandates.
3. **Security and Integrity** – The Agency is responsible for appropriate physical, technical and personnel security measures for maintaining the integrity of the system.
4. **Personnel Changes** –
 - a. The Agency shall use the most current forms or procedures according to KCJIS Policy and Procedures to notify KCJIS of changes to TAC, LASO and Agency Head.
 - b. The Agency shall immediately disable access to KCJIS for any user that is no longer associated with the agency or who will be absent from the agency for more than 60 consecutive days.
 - c. Furthermore, the Agency shall ensure immediate disabling of user access to systems not managed by KCJIS but used to access KCJIS or that may contain criminal justice information (CJI) as defined by KCJIS policy - such as local or regionally shared Computer Aided Dispatch and Records Management Systems.
5. The Agency shall exercise Management Control of all devices and networks utilized to process, store, or transmit CJI as defined in KCJIS policy.
6. **Audit** – The Agency understands they are subject to audit by the administrative agencies of KCJIS and/or the FBI CJIS division for compliance to applicable policies and shall comply with all audit requirements for use of KCJIS and related systems.

The following documents are incorporated by reference and made part of this agreement:

(1) the FBI CJIS Security Policy; (2) KCJIS Administrative Policies and Procedures; (3) the NCIC 2000 Operating Manual; (4) the NLETS Operating Manual, (5) the N-DEx Policy & Operation Manual, (6) the NICS Policy Manual, (7) Title 28, Code of Federal Regulations, Part 20.

The Agency is also subject to applicable federal and state laws and regulations pertaining to criminal justice information use and dissemination. Other policy or operational manuals may be incorporated as access to new systems becomes available through the KCJIS.

Additional conditions and agreements required for participation in certain programs offered through KCJIS may be provided as appendices to this agreement.

KANSAS CRIMINAL JUSTICE INFORMATION SERVICES

AGENCY CONNECTIVITY AGREEMENT

Unless stipulated by statute or otherwise agreed in writing, the Agency shall bear its own costs in relation to this agreement. This agreement in no way implies that the State of Kansas or KCJIS will appropriate funds for such expenditures.

In the event of a security incident or policy violation, the administrative agencies may immediately suspend individual user or Agency access until assurances are made that no threat to KCJIS or CJI exists.

Sanctions for misuse of KCJIS may be levied against individual users or to the Agency. This can include termination of KCJIS services.

The Agency may terminate this agreement upon 30-days written notification to the Kansas Highway Patrol CJIS Unit. In the event of such termination, the following rules apply:

- a. The Agency will continue participation, financial or otherwise, up to the effective date of termination.
- b. The Agency will pay the costs (if any) it incurs as a result of termination.

ACKNOWLEDGMENT AND CERTIFICATION

As an official of the connecting Agency, I hereby acknowledge the duties and responsibilities as set out in this agreement to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained from the KCJIS. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against my agency or users.

I hereby certify that I am familiar with all applicable policies and documents that are made part of this agreement and all applicable federal and state laws and regulations relevant to the receipt and dissemination of information provided through the KCJIS.

This is a formal expression of the intent of the Agency to utilize the KCJIS and is effective when signed. It may be amended after written concurrence between the Agency and representatives of the administrative agencies of the KCJIS.

The "Acknowledgment and Certification" is being executed by an official of the requesting Agency in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the official vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

Agency Head (signature)

Date: _____

Agency Head Name/Title (Please Print)

KCJIS Device Connectivity Request

Agency _____ ORI _____

Name of the Agency Primary TAC: _____ Phone No.: _____

E-mail Address: _____

Name of the Agency LASO: _____ Phone No.: _____

E-mail Address: _____

Name of the I.T. Contact _____ Phone No.: _____

E-mail Address: _____

I.T. Contact Agency or Company Name: _____

Enter the number of NEW devices requested *to be activated within 30 days*

Form factor and PRIMARY FUNCTION of Requested Access Device(s) 	Quantity of devices by Type of Access to NCIC, III, NLets and KS CCH Via the Ks Central Message Switch.		Type of KCJIS Web Portal Services Being Requested <u>NO</u> NCIC, III, or NLets access.
	<u>OpenFox</u>	<input type="checkbox"/> Agency Software <input type="checkbox"/> REJIS Software	
Desktop Computer ⁽¹⁾ for Dispatching (D)			<input type="checkbox"/> Portal Only
Desktop Computer ⁽¹⁾ for Non-Dispatch or Investigations (A)			
Desktop Computer ⁽¹⁾ for TAC Administration (A)		KS Central Message Switch Administration must be done via OpenFox Configurator.	<input type="checkbox"/> KACIS (Qty.) (requires VPN)
Desktop Computer ⁽¹⁾ For Training (T)			<input type="checkbox"/> KSORT (Sheriffs Only)
Mobile Device ^{(2), (3)} (M)		(3)	<input type="checkbox"/> E-disposition (Courts & Prosecutors Only)
eCitation interface ⁽²⁾ (E) (As own device or as a software interface on MDT)	Not Available via OpenFox		
Server ⁽¹⁾ for CAD, MDT, eCitation (If using existing list mnemonic)	Not Applicable to OpenFox		<input type="checkbox"/> Prelog/Case Inquiry

⁽¹⁾ Include KCJIS105 Network Security Questionnaire for all devices on wired network.

⁽²⁾ Include KCJIS229 Mobile Data Device Questionnaire.

⁽³⁾ OpenFox is not available for tablet or smartphones.

KCJIS Network Security Questionnaire

Agency Name _____ ORI _____

LASO Name _____ phone _____

LASO email _____

I.T. Contact _____ phone _____

I.T. email _____ I.T. Agency or Company Name: _____

How does your agency connect to KCJIS? (Check all applicable boxes below.)

State of Kansas Office of Information Technology Services (OITS)
Does your agency have Management Control of a firewall between your network and the OITS network? YES NO

Agency Procured Ground based Internet Service

Agency Procured Wireless Service (complete wireless supplemental questionnaire on page 3)

By way of another Agency or Entity Agency Name: _____

Is access allowed into your network containing CJJ from outside your physically secure location?

None allowed

Remote Access such as vendors or telecommuting¹

Remote Access from branch offices or other agencies¹

¹Please provide agency policies and procedures for when and how remote access is allowed and a KCJIS 232 encryption questionnaire for each remote access method.

Mobile Data Terminals - complete KCJIS229 Mobile Data Device Questionnaire

Other – (describe :) _____

Are there devices in your network that contains CJJ that are used for unsolicited access from the internet or other outside sources (such as e-mail servers, web servers, FTP servers, etc.)? No Yes (show on network schematic)

What network firewall(s) are used? List all models and versions. (See network schematic instructions below). _____

If personal firewalls are used, list brand(s) and version(s): _____

Network Schematic Instructions Please provide a visual representation (schematic) of all wired networks containing CJJ.

1. Do not include any network resolvable addresses or device names.
2. Show a logical summary (don't list all devices) of workstations and servers by physical location groups, VLANs, or virtualized environment (hypervisors), and their connectivity within your local network containing CJJ.
3. Show all logical locations of access points to your network. Include connections to routers, firewalls, wireless access devices, or any other device that provide a path in or out of your network containing CJJ.
4. Indicate connections to non-criminal justice entities such as city or county departments or services like email.
5. Mark "FOR OFFICIAL USE ONLY" on the diagram and include agency name, ORI, and date submitted.

KCJIS Network Security Questionnaire

What brands & versions of Intrusion Detection tools does your agency use? _____

How often are your intrusion detection tools updated? _____

How are your intrusion detection tools updated? _____

Who monitors the intrusion detection tools? _____

What brands & versions of Anti-Virus/Malware protection does your agency use? _____

How often are your Anti-Virus/Malware definition lists updated? _____

Where do your devices get updates to the Anti-Virus/Malware definitions? _____

How often does your Anti-Virus software scan your devices entire hard drive? _____

How does your agency manage patches and updates to devices on your network containing CJI?

Please answer the following questions for all encryption products used by your agency.

KCJIS Provided Encryption

Agency will use the State-supplied SecuRemote client between agency devices and KCJIS. It is understood that, to protect the entirety of KCJIS, any device connected using this option may be disconnected from KCJIS in the event of a security incident involving the device.

Agency will use a site to site VPN configured between Agency network and KCJIS. It is understood that, to protect the entirety of KCJIS, the entire connection using this option may be disconnected from KCJIS in the event of a security incident involving any device

Agency Configured Encryption Product

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

Please complete KCJIS232 Encryption Questionnaire for additional products.

KCJIS Network Security Questionnaire

Wireless Supplemental Questionnaire

Please answer the following questions to determine if your wireless implementation meets the 802.11 Wireless access requirements outlined in FBI and KCJIS policy area 5.13.1.1.

How many Wireless Access Points (WAPs) are in your network that contains CJ? _____
(Please indicate all on the schematic)

Are all WAPs located in physically secure locations? No Yes

Can the WAPs be reached from outside your physically secure facilities? No Yes

What is the approximate range of your WAPs? _____

Has the management interface User ID been changed from factory default? No Yes

Is the management interface User ID unique from other administrative user IDs? No Yes

Do the password attributes for the management interface meet the following requirements?

At least 8 characters	<input type="checkbox"/> No	<input type="checkbox"/> Yes	Expire within 90 days	<input type="checkbox"/> No	<input type="checkbox"/> Yes
Not a dictionary word	<input type="checkbox"/> No	<input type="checkbox"/> Yes	Not any of previous 10	<input type="checkbox"/> No	<input type="checkbox"/> Yes
Not a proper name	<input type="checkbox"/> No	<input type="checkbox"/> Yes	Not transmitted in the clear	<input type="checkbox"/> No	<input type="checkbox"/> Yes
Not the same as the user ID	<input type="checkbox"/> No	<input type="checkbox"/> Yes	Not displayed when entered	<input type="checkbox"/> No	<input type="checkbox"/> Yes

Is the SSID set as the factory default? No Yes

Does the SSID identify the agency or location? No Yes

Is the SSID broadcast? No Yes

List all security features that are enabled on your WAPs: _____

Is the cryptographic module used NIST certified to meet the FIPS 140-2 standards?

No or Not used Yes - NIST cert. # _____ what is the encryption key size used? _____

Have the default encryption keys been changed? No Yes

Has AD HOC mode been disabled? No Yes

Are all nonessential protocols disabled? No Yes

Is HTTP disabled? Yes No If no, is it protected by authentication and encryption? No Yes

Is logging enabled? Not available No Yes

Please indicate on the network schematic how the wireless implementation is separated and insulated from any wired network containing CJ.

Mobile Data Device Questionnaire

Agency Name _____ ORI: _____

TAC Name: _____ Email: _____

LASO Name: _____ Email: _____

Phone: _____

I.T. Contact: _____ Email: _____

Phone: _____ I.T. Agency or Company: _____

1. Does your agency have a written policy for proper use of Mobile Data Devices to mitigate access or viewing of CJJ by unauthorized personnel?

YES

NO

2. Please provide the following information about the device(s) you plan to use:

Laptop or Tablet with Full Featured Operating System (Windows 7, Windows 8.1 Professional, Linux)

i. Operating System, version _____

ii. Antivirus/Antimalware _____

iii. Host based firewall _____

iv. Intrusion Detection solution _____

v. How are devices managed for updates and patches? _____

Smartphone s or Tablet with Limited Featured Operating System (iOS, Android, Blackberry, Windows RT)

i. Device Brand, model: _____

ii. What Operating System and version _____

iii. What MDM solution is used? _____ Version/Build: _____

OTHER device (Please list):

i. Device Brand, model _____

ii. What Operating System and version _____

iii. What MDM solution is used? _____ Version/Build: _____

Add additional sheet if needed to describe all mobile devices being requested.

Mobile Data Device Questionnaire

3. Check all of the possible kinds of network connection(s) the Mobile Device is capable of:

	Connecting types	Can this connection be disabled?			Who/What can manage this connection? (User, MDM,)
		YES	NO	HOW/By Whom	
	Cellular				
	802.11 wireless				
	Radio				
	Wired to local network	X		Unplug by user	
	Other _____.				

4. What is the Password or PIN policy required to uniquely identify users accessing the devices?

Password, PIN, Or NONE	characters or digits required	Dictionary word or proper name allowed?		Repeating digits allowed?		Sequential patterns allowed?		Different than Userid		Expires in #days	History (can't match # previous)	Transmit in clear?		Displayed?	
		YES	NO	YES	NO	YES	NO	YES	NO			YES	NO	YES	NO

5. Is Advanced Authentication required to access local agency systems containing CJI?

- YES - AA solution: _____
- NO

6. How/Where will these mobile devices connect in order to access KCJIS?

- Connect directly to KCJIS using OpenFox and SecuRemote provided by KCJIS (skip 7i.).
- Connect to KCJIS using OpenFox by way of local agency encryption between local networks then site to site to KCJIS (also complete the KCJIS232 encryption questionnaire)
- Connect to a server managed by (local agency) _____
(also complete the KCJIS232 encryption questionnaire).
If EXISTING, what is the server's mnemonic? _____

7. What is the NIST certificate number for the encryption modules used to secure CJI?

- i. Encrypting CJI transmitted between the mobile devices and local systems _____
- ii. Encrypting CJI saved to the mobile device. _____

8. What software is used to access CJI from your mobile device?

Software/Application Name: _____

Software Source/Vendor: _____

KCJIS Encryption Questionnaire

Agency Name _____ ORI: _____

LASO: _____ I.T. Contact: _____

Email: _____ I.T. Email: _____

Phone: _____ I.T. Phone: _____

CJIS Security Policy requires the encryption of Criminal Justice Information (CJI) whenever saved or transmitted outside of Physically Secure Locations as defined in policy. The cryptographic module used must be certified by the National Institute of Standards and Technology (NIST) to meet the Federal Information Processing Standards (FIPS) encryption standard as outlined in FIPS publication 140-2. See the NIST CMVP website <http://csrc.nist.gov/groups/STM/cmvp/index.html> for more information including vendor lists.

Agencies may use products in combination to achieve CJIS security policy compliance. KCJIS and Agency products may be combined. For instance, a Mobile VPN product between MDT and local network can be used along with a site to site VPN to KCJIS for full transmission path encryption. Please note the following:

- SecuRemote may not be compatible for use with servers such as CAD/RMS.
- In the event of a security incident (such as a malware infection) the **connection** used to access KCJIS may be disconnected to protect the entirety of KCJIS, i.e.: single device using SecuRemote or a shared site to site VPN that affects several devices may need disconnected.

Please answer the following questions for all encryption products used by your agency.

KCJIS Provided Encryption

- Agency will use the State-supplied SecuRemote client between agency devices and KCJIS. It is understood that, to protect the entirety of KCJIS, any **device** connected using this option may be disconnected from KCJIS in the event of a security incident involving the device.
- Agency will use a site to site VPN configured between Agency network and KCJIS. It is understood that, to protect the entirety of KCJIS, the **entire connection** using this option may be disconnected from KCJIS in the event of a security incident involving any device

Agency Configured Encryption Product(s)

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ ***at rest*** / or _____ ***in transit*** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

KCJIS Encryption Questionnaire

Agency Configured Encryption Product(s) continued

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** / or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** / or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____
