Criminal Justice Information System (CJIS)

NETWORK SECURITY

A. Access to CJIS sensitive data is only available to authorized users.

B. All CJIS sensitive data shall be encrypted when passing through a public carrier network or any private network not dedicated to Criminal Justice use.

C. Each system user shall have a unique user ID.

D. Each user ID shall have an associated password. Valid passwords shall be at least 6 characters in length and shall consist of both letters and digits. Passwords shall be valid for thirty (30) days.

E. All dial access into the secured CJIS network shall be via the DISC provided dial services. Dial modems are not allowed inside the secured network except as outlined in Technical Policies paragraph 2.E.

F. Specific security standards shall be put into place by each agency regarding the access to the State CJIS system. These standards shall include: Internet Policies, Remote Site Policies, and Mobile Data Terminal (MDT) Policies.

G. The following types of Dial-in-access are permitted from the open CJIS network. Dial access must comply with one of the following. This access must comply with the current version of Paradigm4 CJIS security report, Phase II, paragraph 4.1.1.
1. Locally provided (Modem pool).

2. User accesses through an Internet Service Provider (ISP) as long as it complies with other security policies.

H. Access to the secured CJIS network from the open CJIS network shall occur only through the DISC network firewall.

I. Agency LANs shall provide adequate protection to the CJIS devices on the LAN. This protection may include firewalls or similar access devices as well as server/PC-level access control (logon “ID”, etc.). It is the responsibility of the agency head to ensure that only CJIS-authorized users are able to view CJIS data or issue CJIS transactions.

J. All requests for connection to the open or secure CJIS network shall include a description of how the sites meet the network and technical security policies as defined or the level of connection requested.

PERSONNEL SECURITY (USERS)

An agency with access to CJIS information shall assume responsibility for and enforce CJIS System security policies. Specific personnel security standards shall be met in instances where agencies access the CJIS Network, NCIC and/or III information. Personnel included by the policy include: full time, part time, temporary and contract employees that have access to CJIS systems. These standards are included in the following:

A. No one can have access to the CJIS systems that has been convicted of a felony or severe misdemeanor.

B. All personnel with access must pass a background check minimally including; local name check, State and Federal name and fingerprint check, and local/Federal warrants check, done by the user’s agency.

C. All personnel that have access to the CJIS system shall be at least 18 years old.

D. Upon separation from the Lawrence Police Department the user’s token will be disabled, and/or reassigned to a new user.
E. When accessing the Internet no user shall connect to any web sites pertaining to pornography, including but not limited to downloading of files, viewing material, and transmitting files.

F. All traffic to and from the Lawrence Police Department on the secured CJIS network shall be for Criminal Justice or Law Enforcement business only.

G. After completing a session on the CJIS system the user must shut the system down. Failure to shut down the system will allow unauthorized access. Any unauthorized access to an open system will be identified as the original authorized user.

H. No user shall provide his/her security code to any other person to access the CJIS system, even if the person using the code is an authorized token holder.

I. All policies and procedures apply to Mobile Data Terminals (MDT).

J. Violations of personnel policies and procedures will result in disciplinary action against the user, and can subject the Lawrence Police Department to the loss of the ASTRA system.

K. All authorized users will report their lost or damaged tokens immediately to their supervisor.

PHYSICAL SECURITY

A. The Lawrence Police Department shall ensure all ASTRA terminals and any related CJIS equipment shall have adequate security to protect against unauthorized person(s) gaining access to the computer, network and/or data.

TECHNICAL POLICIES

A. Policies in this section encompass general technical issues involving networks and authentication including management and support of the secured CJIS network and LANs connected to the system.

B. Each work station accessing the system through the KBI KCJIS firewall shall have a unique mnemonic and a valid certificate.
NETWORK MANAGEMENT, DIAGNOSTICS, AND REPAIR

A. DISC shall be responsible to ensure the 7x24 availability of the secured and open CJIS networks, in accordance with the service level agreement(s) implemented between DISC and the Kansas Criminal Justice Coordinating Council.

B. Third party vendors, consultants, etc., employed to perform maintenance or network service shall be monitored. It shall be the responsibility of the criminal justice agency to ensure no CJIS sensitive data is allowed to leave the site without prior approval. A log of CJIS sensitive data which has left the site shall be maintained for two (2) years.

ACCESS TO SECURED CJIS NETWORK

A. Only criminal justice agencies with no other non-criminal justice agency on their LAN and/or WAN shall access the CJIS system.

B. A LAN connected to the secured CJIS network shall have only one access point to or from the LAN; that being the router connection to the secured CJIS network.

C. Traffic to or from an agency on the secured CJIS network shall be for criminal justice or law enforcement business purposes only. It is the responsibility of the Lawrence Police Department to ensure compliance with this policy.

D. Any dial access shall be authenticated and logged at the time of connection. All backups or other copies of CJIS information taken from the CJIS servers shall be protected to ensure no unauthorized access to the data is possible if removed from the secured physical location.

E. No modems shall be permanently connected to the LAN on the secured CJIS network. Controlled modem access is permitted when the modem is enabled only during the time the dial in was necessary and immediately disabled.

F. DISC may employ additional monitoring as necessary to isolate network problems on the secured and open CJIS networks. With the owning agency’s approval DISC may employ additional
monitoring as necessary to isolate network problems that appear to be originating from a local LAN.

TRAINING POLICIES

All CJIS terminal users should be trained to their level of access within six (6) months of employment. The following outlines the training that each level of personnel shall achieve.

A. All FULL ACCESS operators shall pass the NCIC certification test given by the Kansas Highway Patrol. This certification shall be renewed every two years. If certification expires, the operator will not be allowed on the network until re-certification is completed.

B. All LESS-TAN-FULL-ACCESS operators shall be tested by the employing agency, and re-tested every two years to ensure operators’ proficiency. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits. In addition, the Kansas Highway Patrol shall be notified of the names of all LESS-TAN-FULL-ACCESS operators, and the dates of their certification.

C. All sworn law enforcement personnel shall receive basic training in NCIC matters adhering to the minimum curriculum recommended by the NCIC in order to ensure effective use of the system and compliance with the NCIC policies and regulations. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits.

D. The agency shall provide training to the level of access permitted for CRIMINAL JUSTICE PRACTITIONERS. This would include such personnel as record clerks, court clerks, district attorneys, etc. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits.

E. Within six (6) months of election, selection or assignment, CRIMINAL JUSTICE ADMINISTRATORS and upper level supervisory personnel shall obtain training concerning capabilities of the CJIS Network, regulations, policy, audit requirements, sanctions, and related civil liability problems. The training is designed to familiarize administrators with the key issues that affect their agency. The employing agency shall keep
documentation of all training that it provided and documentation shall be provided during audits.

F. All personnel assigned to technical and supervisory positions with access to the CJIS system shall have received approved training within six (6) months of their appointment.

All personnel with CJIS access shall be trained on privacy and security issues regarding criminal history record information. Once trained, all personnel shall sign awareness statements showing that they understand the penalties and/or circumstances of misusing Criminal History Record Information (CHRI).

All CJIS terminal users should be provided network security awareness training within six (6) months of employment.

ADMINISTRATIVE SECURITY POLICIES

A. RECORD KEEPING- Each agency is held responsible for their record keeping practices. This information will be monitored through compliance audits.

B. DESTRUCTION/DISPOSAL- All information received from the CJIS Network shall be destroyed when no longer needed.

C. DOCUMENTATION- Documentation that supports any operations on the CJIS Network, training personnel security violations, etc., shall be provided to authorized audit staff upon request.

D. NOTIFICATION- If a violation of security is discovered the discovering agency shall notify the state NCIC Control Terminal Officer (CTO) without delay. Immediate reporting of such violation is expected. In any event, the discovering agency shall ensure that the state NCIC CTO is notified of such violation within one business day

E. ADMINISTRATION- Each agency shall appoint a Terminal Agency Coordinator (TAC) who shall serve as a focal point for the CJIS issues, including these administration policies.

AUDIT POLICY

The Kansas Criminal Justice Coordinating Council (KCJCC), the Federal Bureau of Investigation (FBI), the Criminal Justice Information System (CJIS) Advisory Board, and the Kansas Law Enforcement Telecommunications Committee (ASTRA), have charged the Kansas Bureau of Investigation (KBI) and the Kansas Highway Patrol (KHP) with the audit responsibilities for the CJIS Network.
Those responsibilities are created through the following statutes, rules and regulations and/or policies:

1. FBI Security Policy
2. K.S.A. 22-4704
3. K.S.A. 74-5701
4. K.S.A. 74-5702

Periodically, the KBI and/or the KHP will conduct audits to ensure compliance with established policies. During on-site audits at least the following areas may be reviewed:

1. Network Security
2. Personnel Security
3. Physical Security
4. Technical Security
5. Training Issues
6. Administrative Security

Additional areas may also become part of the periodic audits that are not included in the policies listed above. Those areas are listed below.

1. Information Quality
2. Dissemination
3. Validation Review
4. NCIC Quality Assurance
5. Kansas Hot Files Quality Assurance

Each agency shall respond to the NCIC CTO or his designee, in writing within thirty (30) days of receiving any final audit report, where an area is non-compliant.

If areas of non-compliance are not corrected the report will be referred to the NCIC CTO, who will determine the appropriate sanctions, or termination of service.

As a result of the auditor’s findings and recommendations outlined in the final report, sanctions may be recommended to the NCIC Control Terminal Officer. The CTO will notify the local agency of any sanctions or other required change.