

Management Control Agreement

Pursuant to the CJIS Security Policy Version 5, Sections 3.2.2 and 5.1, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel.
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“Responsibility for management of security control shall remain with the criminal justice agency.”

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date _____

Joan Brown, CIO
(Criminal Justice Agency)

Date _____