Management Control Agreement

BETWEEN
The Florida Department of Juvenile Justice (DJJ)
And
Miami-Dade County Information Technology Department (ITD)
For
Providing Criminal Justice Information Technology Services

PURPOSE:
This Management Control Agreement (MCA) is between the ***Florida Department of Juvenile Justice (DJJ)*** and the ***Miami-Dade County Information Technology Department (ITD)***. This agreement covers the overall supervision of technical services provided by ITD on behalf of ***DJJ*** for data transport (network) services used to access equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of DJJ system to include the National Crime Information Center (NCIC) and the Florida Crime Information Center (FCIC) programs that may be subsequently designed and/or implemented within DJJ

Pursuant to the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services' (CJIS) Security Policy Version 5, 02/09/2011, 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 located within the Children's Courthouse, hereafter referred to as CCH for the interstate exchange of criminal history/criminal justice information, the ***Florida Department of Juvenile Justice,*** hereafter referred to as ***DJJ*** shall have the authority, via managed control to set:

1) CJIS priorities regarding the access, use, and maintenance of CJIS IT equipment used for transporting and processing FBI CJIS data.
2) Standards consistent with CJIS policy for the selection, supervision and termination of personnel who have virtual and physical access to the aforementioned IT equipment, as outlined in this document, the DJJ/FDLE CJIS User Agreement and the FBI CJIS Security Policy.
3) Management controls governing, operation of access devices, circuits, hubs, routers, firewalls, and any other components, 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, as dictated and defined in the DJJ/FDLE CJIS User Agreement and the FBI CJIS Security Policy.
4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
5) Compliance with all rules and regulations of ***DJJ*** IT and CJIS Security Policies in reference to the access, use, storage and maintenance of CJIS IT equipment and CJIS data.

"Responsibility for management of security control shall remain with the criminal justice agency" CJIS Security Policy Version 5.0, February 9, 2011, Section 3.2

WHEREAS, ***DJJ*** is a recognized Criminal Justice Agency (CJA) and ITD is a Non-Criminal Justice Agency (NCJA) designated to provide information technology (IT) support services for the ***DJJ;***

WHEREAS, The ***DJJ*** presently has executed a Criminal Justice User Agreement with the Florida Department of Law Enforcement, hereafter referred to as FDLE, for the benefit of access to the Florida Criminal Justice Network (CJNet), the National Crime Information Center (NCIC) and the Florida Crime Information Center (FCIC);

WHEREAS, the FBI requires an agreement to document security requirements for the ITD (a NCJA) to provide technical support services to ***DJJ*** (a CJA) for DJJ's computer systems and network infrastructure that directly or indirectly interfaces with the ITD computer systems and network infrastructure;

WHEREAS, ITD has be designated to provide technical support to the ***DJJ,*** including housing and maintaining IT equipment (i.e. routers, switches, wireless access points, etc.) that may be used for processing or transmitting FBI and/or FDLE criminal justice information;

NOW THEREFORE, The parties agree as follows,

1. ITD agrees to abide by the terms and conditions of the Criminal Justice User Agreement executed into between the FDLE and the ***DJJ*** (Attached as Exhibit 1).

2. ITD agrees to abide by the requirements of the FBI CJIS Security Policy (Attached as Exhibit 2).

3. The ***DJJ*** retains Security Control, as defined in the FBI CJIS Security policy, of the technical support functions for CJIS data and equipment provided by ITD.

4. All ITD staff who are authorized to maintain/support NCIC/FCIC/CJNet information technology components (this includes, routers, switches and/or any other components used to process, or transmit NCIC/FCIC/CJNet data) on behalf of the ***DJJ*** are required to undergo a DJJ background investigation, prior to being granted access to the aforementioned components.

5. The terms of this agreement shall be continuous; commencing on the date the agreement is signed.

6. Either party may terminate the agreement upon thirty (30) days written notice, except that the ***DJJ*** may terminate this agreement immediately and without notice upon finding that there has been violation to the terms of this agreement.

7. This agreement constitutes the entire agreement of the parties and may not be modified or amended without written agreement executed by both parties.

IN WITNESS HEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

Criminal Justice Agency (CJA) Name: Department of Juvenile Justice (DJJ)

CJA CIO: _____ **Dated:** 6/19/2015

Witness: _____ **Dated:** 6/19/2015

Non-Criminal Justice Agency (NCJA) Name: Miami-Dade County ITD

NCJA CIO: _____ **Dated:** 6/17/15

Witness: _____ **Dated:** 6/17/15