MANAGEMENT CONTROL AGREEMENT

BETWEEN

ST. LUCIE COUNTY SHERIFF'S OFFICE, FORT PIERCE POLICE DEPARTMENT, PORT ST. LUCIE POLICE DEPARTMENT

AND

ST. LUCIE COUNTY

FOR THE PURPOSES OF
PROVIDING CRIMINAL JUSTICE INFORMATION TECHNOLOGY SERVICES, INFORMATION EXCHANGE, DISPATCH SERVICES, AND CRIMINAL JUSTICE AGENCY OVERSIGHT

WHEREFORE, the Management Control Agreement (Agreement) by and between St. Lucie County Sheriff's Office, hereinafter referred to as the Oversight Agency (OA), and St. Lucie County through its 911 Center, hereinafter referred to as DISPATCH establishes and identifies the specific roles that each party shall fulfill. This Agreement provides guidelines for the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI), pursuant to the Federal Bureau of Investigations (FBI) Criminal Justice Information Systems (CJIS) Security Policy (CJISSECPOL). Further, this Agreement also outlines the roles and responsibilities of each party in relation to DISPATCH personnel screening and training, DISPATCH third-party vendor requirements, DISPATCH adherence to the FBI CJIS Security Policy Security Addendum Process, and general oversight responsibilities.

This Agreement applies to every individual, contractor, vendor, private entity, non-criminal justice agency representative, and/or member of the OA and the DISPATCH.

NOW, THEREFORE, in consideration to the mutual promises and covenants herein, the Parties hereby agree as follows:

I. ACCESS TO CRIMINAL JUSTICE INFORMATION

a. DISPATCH is a county department that performs a criminal justice function for the OA.

b. DISPATCH shall meet the minimum requirements as outlined by the FBI CJIS Security Policy in regards to access, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information.

c. DISPATCH shall not disseminate any Criminal Justice Information to any entity other than the OA and the Law Enforcement Agencies outlined within this Agreement.

d. DISPATCH shall not enter into any contracts with other Criminal Justice Agencies or Non-Criminal Justice Agencies for the exchange of Criminal Justice Information. All agreements for exchange of CJI must be between the OA and another criminal justice agency on behalf of DISPATCH.

e. DISPATCH shall appoint a Local Agency Coordinator (LASO) who will work with the LASO of the OA. The LASO shall ensure that all technical controls to secure Criminal Justice Information are in place and in working order.

f. In the event of a network intrusion or breach to Criminal Justice Information, the LASO shall contact the LASO of the OA and report the intrusion or breach immediately.

II. DISPATCH PERSONNEL VETTING

a. All DISPATCH staff that have physical and/or logical access to the DISPATCH building and/or network must undergo a fingerprint-based records check under the OA's Originating Agency Identifier (ORI). These records will be retained by the OA until such a time that an individual is no longer working for DISPATCH. The fingerprint-based records check must occur prior to granting access to the DISPATCH building and/or network.

b. The OA will provide guidance to DISPATCH if an individual does not meet the requirements for access or if a retained individual is arrested during their employment.

c. The DISPATCH is required to have a Florida Crime Information Center (FCIC) Agency Coordinator (FAC) who will work with the FAC from the OA to ensure each individual with physical or logical access, has and maintains, current Security Awareness Training and/or Limited/Full Access Training. All individuals must have current training within six months of assignment.

III. DISPATCH VENDORS AND CONTRACTORS

a. All DISPATCH vendors and contractors that have physical and/or logical access must undergo a fingerprint-based records check under the OA's ORI. These records will be retained by the OA until such a time that the vendor/contractor personnel no longer have access. The fingerprint-based records check shall occur prior to gaining physical or logical access.

b. The OA will provide guidance to DISPATCH if an individual from the DISPATCH vendor/contractor does not meet the requirements for access or if vendor/contractor personnel are arrested during their employment.

c. The DISPATCH FAC will ensure that all vendor/contractor personnel have the required level of training based off of the work they are performing. The DISPATCH FAC will work with the OA FAC to ensure all training is complete and kept current.

d. The OA reserves the right to terminate this agreement, with or without notice, upon determining DISPATCH or DISPATCH personnel have violated any applicable law, rule of regulation or has violated the terms of this agreement.

IV. OVERSIGHT AGENCY RESPONSIBILITIES

The OA is responsible for the following in terms of compliance with the FDLE User Agreement and FBI CJIS Security Policy:

a. Ensuring that the DISPATCH has designated a FAC and LASO and that all associated trainings for those positions has occurred.

b. Ensure all DISPATCH personnel and DISPATCH vendors/contractors are retained under the OA's ORI.

c. Ensure that Access Reviews are done on behalf of DISPATCH.

d. Work with DISPATCH FAC and LASO to ensure all DISPATCH personnel and DISPATCH vendors/contractors have and maintain current training.

e. Maintain a signed Security Addendum Certification Page for all DISPATCH personnel and vendor/contractor personnel.

f. Ensure that Criminal Justice Information is secured throughout its lifecycle.

g. Ensure that DISPATCH does not run driver's license, Criminal History Record Information (CHRI), tag checks, etc., for any other entity other than the OA and other Law Enforcement Agencies that are named in this Agreement.

h. Ensure that the OA LASO and/or FAC is available for any audits conducted on the DISPATCH site.

V. MANAGEMENT CONTROL OF INFORMATION TECHNOLOGY SERVICES ON BEHALF OF THE OA AND DISPATCH

This Agreement also covers the overall supervision of technical services provided by St. Lucie County Information Technology Department on behalf of the St. Lucie County Sheriff's Office for data transport, network services used to access equipment, systems design, programming and operational procedures associated with the development, implementation, and maintenance of the St. Lucie County Sheriff's Office systems to include the National Crime Information Center (NCIC) and the FCIC programs that may be subsequently designed and/or implemented within the St. Lucie County 911 Center.

Pursuant to the CJIS Security Policy, 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 (FCIC/NCIC) located within the EOC for the interstate exchange of criminal history/criminal justice information, the St. Lucie County Sheriff's Office shall have the authority, via managed control, to set, maintain, and enforce:

(1) **Priorities**. In the event of a County-wide infrastructure failure, the St. Lucie County Information Technology Department will work to ensure that the County Law Enforcement network services are restored as a priority to ensure public safety response as needed.

(2) **Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI)**. The St. Lucie County Information Technology Department will provide St. Lucie County Sheriff's Office a list of personnel who will have physical and/or logical access to the network accessing, processing, storing or transmitting CJI. Prior to giving those individuals access to the network or any component thereof, the individual will have a fingerprint-based record check completed under the St. Lucie County Sheriff's Office's ORI and Security Awareness Training. If the St. Lucie County Information Technology Department terminates a member of the Information Technology Team, the St. Lucie County Sheriff's Office will be notified and all rights and privileges for that individual will be immediately revoked. The St. Lucie County Information Technology Department will update and keep current a list of individuals with access and provide that to the St. Lucie County Sheriff's Office any time a change occurs.

(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**. The St. Lucie County Information Technology Department will ensure the St. Lucie County Sheriff's Office/St. Lucie County 911 Center network is monitored at all times for any security related incidences or intrusions. If found, the St. Lucie County Information Technology Department will notify the St. Lucie County Sheriff's Office immediately and work to contain the breach and limit the loss of data or system integrity. If the St. Lucie County Information Technology Department outsources to a third-party vendor, they will consult with the St. Lucie County Sheriff's Office for guidance regarding personnel vetting and access prior to allowing the third-party any physical or logical access to the criminal justice network and/or physically secured location.

(4) **Restriction of unauthorized personnel from access or use of equipment accessing the State network**. St. Lucie County Sheriff's Office will monitor and control all access to the network and/or criminal justice information (CJI) System. Access will only be given to those individuals that have been approved in the selection process. St. Lucie County Sheriff's Office will also terminate access to any vetted personnel who voluntary/involuntary leaves the agency.

(5) **Compliance with all rules and regulations of the St. Lucie County Sheriff's Office Policies and CJIS Security Policy in the operation of all information received**. The St. Lucie County Information Technology Department will comply with all rules, regulations and procedures outlined by the St. Lucie County Sheriff's Office and the CJIS Security Policy in regard to personnel and the maintenance and upkeep of the criminal justice network.

(6) General Services:

a. St. Lucie County Information Technology Department agrees that only authorized St. Lucie County Information Technology Department personnel will conduct and/or witness the destruction of devices used to access, process, and/or store criminal justice information.

b. St. Lucie County Information Technology Department will escort vendor personnel who may have access to St. Lucie County Sheriff's Office/ St. Lucie County 911 Center's hardware and/or software, or to the physical location of such hardware.

c. St. Lucie County Information Technology Department will confer with St. Lucie County Sheriff's Office prior to implementing any technologies or utilizing a vendor that is not currently under contract with the Sheriff's Office prior to providing any access to the network or network components.

d. Vendors under contract with St. Lucie County that provide access and/or services to St. Lucie County Sheriff's Office must adhere to the requirements as outlined within the FBI CJIS Security Policy Security Addendum Process as outlined in Appendix H of the FBI CJIS Security Policy.

e. St. Lucie County Fire District has access to the Criminal Justice CAD. The devices utilized to access the CAD must meet the requirements of the CJISSECPOL and the FDLE User Agreement. St. Lucie County Information Technology Department will work with the Information Technology group utilized by St. Lucie Fire District in order to ensure this requirement. St. Lucie County Fire District personnel must undergo a fingerprint-based record check under the St. Lucie County Sheriff's Office ORI and maintain current security awareness training.

It is further understood that "…*management control of the criminal justice function remains solely with the Criminal Justice Agency*." As per Section 5.1.1.4 of the CJIS Security Policy.

This Agreement also covers the overall supervision of all St. Lucie County Sheriff's Office systems, services, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any St. Lucie County Sheriff's Office system to include FCIC and NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

VI. ACCESS TO CJI SYSTEMS/APPLICATIONS AND SERVICES PROVIDED

(1) DISPATCH will facilitate dispatching functions for the OA, the Fort Pierce Police Department (FPPD), and the Port St. Lucie Police Department (PSLPD).

(2) DISPATCH will facilitate dispatching functions for the St. Lucie County Fire District (SLCFD).

(3) DISPATCH hosts the Computer Aided Dispatch (CAD) and the OA's Record Management System (RMS).

(4) Access to the CAD and RMS will be provided to the OA, FPPD, and PSLPD via site-to-site encrypted tunnels. SLCFD Personnel have access to the FIRE Module of the CAD interface only. The access is via a FIPS 140-2 encrypted path.

(5) Additional exchange of CJI between parties include Voice and Physical Paper Exchange.

(6) Each agency will be provided with Audit Logs for their users on a weekly basis for the CAD and RMS. Each agency will review their own logs as required by the FBI CJIS Security Policy.

(7) The OA maintains managed control of the CAD and RMS as related to FDLE and FBI CJIS requirements.

(8) All parties agree to abide by applicable federal and state laws as well as the terms and conditions of the Criminal Justice User Agreement executed between FDLE and the respective agencies.

(9) All parties agree to make, use, and disseminate CJI related records for authorized criminal justice purposes only and maintain any information in a secure place. All destruction of CJI related information will follow all applicable federal and state laws.

IN WITNESS WHEREOF, is hereby agreed that the terms and conditions contained in this Management Control Agreement have been accepted by the officials signed names below, who are bound by the terms and conditions of this Management Control Agreement.

ST. LUCIE COUNTY SHERIFF

BY: _____

DATE: _____

APPROVED AS TO FORM AND CORRECTNESS:

_____

General Counsel

ATTEST:

_____
Linda Cox, City Clerk

CITY OF FORT PIERCE:

BY: _____
Linda Hudson, Mayor

DATE: _____

FORT PIERCE POLICE DEPARTMENT:

_____
Diane Hobley-Burney, Chief

DATE: _____

APPROVED AS TO FORM AND CORRECTNESS:

_____
Sara K. Hedges, City Attorney

ATTEST:

City Clerk

CITY OF PORT ST. LUCIE POLICE DEPARTMENT

BY: _____

Chief

DATE: _____

APPROVED AS TO FORM AND CORRECTNESS:

_____

City Attorney

ATTEST:

Deputy Clerk

ST. LUCIE COUNTY, FLORIDA

BY: _____

County Administrator

DATE: _____

APPROVED AS TO FORM AND CORRECTNESS:

_____

County Attorney

WITNESSES:

ST. LUCIE COUNTY FIRE DISTRICT CHIEF

BY: _____

DATE: _____

APPROVED AS TO FORM AND CORRECTNESS:

_____

District Attorney