MANAGEMENT CONTROL AGREEMENT BETWEEN ORLANDO POLICE DEPARTMENT, GREATER ORLANDO AVIATION AUTHORITY- AIRPORT EMERGENCY COMMUNICATIONS CENTER, AND CITY OF ORLANDO TECHNOLOGY MANAGEMENT

THIS Management Control Agreement is entered into by and between: THE ORLANDO POLICE DEPARTMENT a law enforcement department, within the City of Orlando, hereinafter referred to as "OPD."

AND

GREATER ORLANDO AVIATION AUTHORITY – AIRPORT EMERGENCY COMMUNICATIONS CENTER, a non-criminal justice entity, having its own ORI, providing a criminal justice function, under the oversight of a criminal justice agency, "OPD", hereinafter referred to as "GOAA."

AND

CITY OF ORLANDO INFORMATION TECHNOLOGY, a department within the City of Orlando hereinafter referred to as "IT."

WHEREAS, "OPD" operates a police department that performs the administration of criminal justice; and

WHEREAS, "GOAA" performs a criminal justice function (dispatching) under the oversight of "OPD" by utilizing network components, hardware, and software of the "OPD Trust" criminal justice network; and

WHEREAS, "IT" performs the administration of assessment, installation, and maintenance of computer systems for the City, to include "OPD" and "GOAA".

WHEREAS, "OPD Trust" is a segregated area separating Criminal Justice Information Services (CJIS) systems and traffic from other City systems via a firewall that requires a second form of identification.

WHEREAS, the parties desire to enter into a Management Control Agreement;

NOW THEREFORE AND IN CONSIDERATION of the mutual terms, conditions, promises, and covenants, hereinafter set forth, the parties agree as follows:

Pursuant to the CJIS Security Policy Version 5.8, Section 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 OPD Trust for the interstate exchange of criminal history/criminal justice information, the Orlando Police Department shall have the authority, via managed control, to set and enforce:

1. Priorities: CJIS priorities regarding the access, use, and maintenance of CJIS equipment used for transporting and processing FBI CJIS data. The Orlando Police Department will have authority to set and enforce priorities within the OPD Trust where law enforcement or criminal justice information matters are involved.

2. Standards for the selection, supervision and termination of personnel. GOAA and IT will provide OPD with a list of personnel who will have physical and/or logical access to the network accessing, processing, storing and/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 OPD ORI and the appropriate level of security awareness training and/or CJIS training. If GOAA and/or IT terminate a member of the dispatch center or information technology team, OPD will be notified and all rights and privileges for that individual will be immediately revoked. GOAA and IT will update and keep current a list of individuals with access and provide that to OPD 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 the network infrastructure 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. IT will ensure the OPD Trust is monitored for any security related incidences or intrusions. If found, IT will notify OPD immediately and work to contain the breach and limit the loss of data or system integrity. If IT outsources to a third-party vendor, they will consult with OPD for guidance regarding personnel and access prior to allowing the third party any physical or logical access to the criminal justice network.

4. Restriction of unauthorized personnel from access or use of equipment accessing the State network. Any individual that works directly or indirectly with GOAA and/or IT who fails to maintain up-to-date Security Awareness training or whose fingerprint based record check reveals a felony of any kind, that individual will be denied physical and logical access to CJI until a review by the CJIS Systems Officer (CSO) or designee is either approved or denied.

5. Compliance with all rules and regulations of the Orlando Police Department policies and CJIS Security Policy in the operation of all information received. GOAA and TM will comply with all rules, regulations and procedures outlined by OPD and the CJIS Security Policy in regards to personnel and the maintenance and upkeep of the criminal justice network.

6. TM will be responsible for the destruction and sanitization of all devices from the OPD Trust network and will ensure that the sanitization and destruction is carried out by individuals who have been fingerprinted and trained under the OPD ORI.

7. OPD will partner with IT to review/analyze information system audit records for indications of inappropriate or unusual activity for CJI systems, and to investigate suspicious activity or suspected violations. If IT suspects improper or suspicious activity, IT will notify the OPD FAC and take the necessary actions. If the activity is associated with a GOAA user, the OPD FAC will notify the GOAA LASO.

"Responsibility for management of security control shall remain with the criminal justice agency." CJIS Security Policy Version 5.8 Section 3.2.

Overall responsibility for management of security control shall remain with the Orlando Police Department.

This agreement covers the overall supervision of all Orlando Police Department systems, applications, equipment, systems design, programming and operational procedures associated with the development, implementation and maintenance of any Orlando Police Department system to include NCIC Programs that may be subsequently designed and/or implemented ,within the Orlando Police Department criminal justice network.

AGREEMENT PERIOD

The Parties agree that this Management Control Agreement shall be in full force, upon the last party to sign this Management Control Agreement. Either party may terminate this Management Control Agreement by providing the other party with five (5) days written notice. Notice may be delivered by email and will be effective on the date that it is given. The Management Control Agreement may be modified upon joint agreement of both parties. It 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.

WITNESSES:

By:______________________________________

Printed Name:____________________________

By:______________________________________

Printed Name:____________________________

CITY OF ORLANDO, ORLANDO POLICE
DEPARTMENT

By:________________________________

Printed Name: Orlando Rolón

Title: Chief of Police

WITNESSES:

By:_________________________________
Printed Name:_________________________

By:_________________________________
Printed Name:_________________________

CITY OF ORLANDO, INFORMATION
TECHNOLOGY

By:_____________________________
Printed Name: Rosa Akhtarkhavari
Title: Chief Information Officer

WITNESSES:

By:_______________________________

Printed Name:_____________________

By:_______________________________

Printed Name:_____________________

GREATER ORLANDO AVIATION AUTHORITY

By:___________________________

Printed Name: Phillip N. Brown
Title: Chief Executive Officer

Approved as to Form and Legality on the
_____ day of _____________, 2020,
for the use and reliance of the
Greater Orlando Aviation Authority only.

By: ______________________________
Marchena and Graham, P.A.