CRIMINAL JUSTICE USER AGREEMENT

This Agreement, is entered into between the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the State of Florida with headquarters at 2331 Phillips Road, Tallahassee, Florida and the

Orlando Police Department,

with headquarters at
100 South Hughey Avenue, Orlando, Florida 32801,

with the primary ORI of: FL0480400, (hereinafter referred to as the User).

Whereas, FDLE is authorized by law to operate and regulate the Florida Criminal Justice Network (hereinafter CJNet) as an intra-agency information and data-sharing network for use by the state's criminal justice agencies;

Whereas, FDLE is authorized by law to establish and operate the Florida Crime Information Center (hereinafter FCIC) for the exchange of information relating to crimes, criminals and criminal activity;

Whereas, FDLE participates in the National Crime Information Center (hereinafter NCIC), a service of the United States Department of Justice, the Interstate Identification Index (hereinafter III), the Federal Bureau of Investigation's (hereinafter FBI) Law Enforcement Online (hereinafter LEO), the FBI's National Data Exchange (hereinafter NDEx) and the International Justice and Public Safety Network (hereinafter Nlets), and serves as Florida's Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the interstate transmission of Criminal Justice Information (CJI) to and from agencies in Florida and agencies in the continental United States, Alaska, Hawaii, U.S. Virgin Islands, Canada and Puerto Rico;

Whereas, the FDLE Director of Criminal Justice Information Services is recognized by the FBI as the CJIS Systems Officer (CSO) for the State of Florida, responsible for administering and ensuring statewide compliance with the FBI CJIS Security Policy (CSP);

Whereas, the User requires access to intrastate and interstate CJI systems provided by FDLE through the CJNet in order to effectively discharge its public duties;

Whereas, FDLE facilitates local law enforcement and other criminal justice agencies' requests to participate in the information services provided on CJNet, provided the User agrees to abide by applicable federal and state laws; administrative code, and all policies, procedures and regulations related to these systems. FDLE retains full control over the management and operation of CJNet and FCIC.

Therefore, in consideration of the mutual benefits to be derived from this Agreement, the FDLE and the User do hereby agree as follows:

This User Agreement is designed for criminal justice agencies within Florida that have either direct or indirect access to FCIC/CJNet. If the User does not perform a specific function, the provisions regarding that function will not apply to the User.

SECTION I FCIC/NCIC/CJNET FDLE REQUIREMENTS

FDLE is duly authorized and agrees to ensure access to the criminal justice information services provided on CJNet and adhere to the following:

1. Serve as the CSA for the State of Florida and provide the User with access to CJI as is available in the FCIC/NCIC and III systems and NLETS through CJNet, and to serve as the means of exchanging CJI between the User and other criminal justice agencies on CJNet.

2. Provide the opportunity for CJIS certification/re-certification and CJIS Security Awareness training.

3. Provide the User with information concerning privacy and security requirements imposed by state and federal policies, laws, rules and regulations. All references herein to policies, operating procedures, operating instructions, operating manuals and technical memoranda with which adherence is required may be found on the CJNet CJIS Resource Center web page.

4. Provide state criminal history record check services for non-criminal justice purposes as provided by law.

5. Act as the central state repository; provide identification, record keeping, and exchange of Criminal History Record Information (CHRI) services.

6. Facilitate access, using CJNet, to other information applications or systems that the User may be authorized to access.

SECTION II FCIC/NCIC/CJNET USER REQUIREMENTS

By accepting access as set forth above, the User agrees to adhere to the following to ensure continuation of access:

1. USE OF THE SYSTEM: **Use of the CJNet and any system accessed via the CJNet is restricted to the administration of criminal justice or as otherwise specifically authorized or required by statute.** Information obtained from the FCIC/NCIC files, or computer interfaces to other state or federal systems, by means of access granted through CJNet, can only be used for authorized purposes in compliance with FCIC/NCIC and III rules, regulations and operating procedures, and state and federal law. It is the responsibility of the User to ensure access to CJNet is for authorized purposes only, and to regulate proper use of the

network and information at all times. The User shall establish appropriate written standards, which may be incorporated with existing codes of conduct, for disciplining violators of this and any incorporated policy. Accessing information and systems provided via CJNet for other than authorized purposes is deemed misuse. The User shall notify the CSO of any sustained/confirmed cases of misuse by using the CJS Systems Misuse Reporting Form found on the CJNet CJIS Resource Center web page. In cases of sustained/confirmed misuse, the User shall identify disciplinary actions and the corrective actions taken to prevent future incidents. FDLE reserves the right to deny CJI access to individuals who have sustained cases of misuse.

1.1 If the User provides an interface between FDLE and other criminal justice agencies, the serviced agency(ies) shall abide by all of the provisions of this agreement. Serviced agencies that access CJNet, FCIC/NCIC and/or related applications by interfacing through the User shall, likewise, abide by all provisions of this agreement. Additionally, the User and the serviced agency shall enter into an interagency agreement when access to CJNet/FCIC/NCIC is provided by the User to a serviced agency.

1.2 MESSAGES: Only law enforcement and other criminal justice messages shall be sent over and through the CJNet and FCIC/NCIC. All messages shall be treated as privileged unless otherwise indicated. The User should be prudent in use of regional and statewide broadcast message requests. All messages shall use plain English language in the message.

1.3 COMPLIANCE: The User shall access FCIC/NCIC and other CJNet applications in strict compliance with applicable CJNet, FCIC, NCIC, III and Nlets policies including, but not limited to, policies, practices and procedures relating to:

1.3.1 TIMELINESS: FCIC/NCIC records shall be entered, modified, located, cleared, and canceled promptly in order to ensure system accuracy and effectiveness. If the User performs FCIC/NCIC updates for other agencies, the User shall comply with timeliness requirements for the records entered for the serviced agencies as well.

1.3.2 HOT FILE ENTRIES: In order to make entries into the FCIC/NCIC hot files, the User shall have personnel dedicated to maintain a 24-hour, seven-day a week FCIC/NCIC operation.

1.3.2.1 If the User enters records into FCIC/NCIC for another agency, the User shall execute an interagency agreement with each serviced agency outlining each agency's responsibilities.

1.3.2.2 Adult Warrants, Missing Persons and all property records of the FCIC Hot File records, entered by state and local agencies, will be made available to the public on the Internet via the FCIC Public Access System (PAS), unless explicitly flagged by the User for exclusion.

1.3.3 QUALITY ASSURANCE: Appropriate and reasonable quality assurance procedures shall be in place, including second party verification during entry, to ensure all entries in FCIC/NCIC are complete, accurate, and valid.

1.3.4 VALIDATION: The User shall validate all records that the User has entered into the system for accuracy and retention. To be in compliance with FCIC/NCIC rules, regulations and operating procedures, the User shall ensure each record is modified to confirm the successful validation of each record on file in FCIC/NCIC. Failure to modify a record to indicate validation may result in its removal from the file. The User shall develop its own written validation procedures specifying the steps taken by the User to complete record validation.

1.3.5 HIT CONFIRMATION: The User shall comply with FCIC/NCIC rules, regulations and operating procedures by responding to the hit confirmations in a timely manner (within ten minutes or one-hour depending on priority).

1.3.6 DISSEMINATION: Information obtained from the FCIC/NCIC hot files, CJNet or computer interfaces to other state or federal systems, by means of access granted pursuant to Section 943.0525, F.S., shall only be used for the administration of criminal justice.

1.3.6.1 Upon receipt of a public record request for CJI, the User shall confer with FDLE regarding the appropriate response. It is the responsibility of the User to ensure that access to the CJNet is for authorized criminal justice purposes only, and to regulate proper access to and use of the network and information at all times.

1.3.6.2 The User will disseminate CHRI obtained or derived from federal records or systems only to criminal justice agencies and only for the administration of criminal justice. The administration of criminal justice includes criminal justice employment screening.

1.3.6.3 The User, if functioning in the capacity of a pretrial release program or providing CHRI for a pretrial release program, may disseminate Florida public record information only, in compliance with Section 907.043 (3),

F.S., which requires "[e]ach pretrial release program [to] prepare a register displaying information that is relevant to the defendants released through such a program." The authority to disseminate information for this purpose shall be restricted to county probation services offices and those criminal justice entities providing the probation offices with information obtained via the FCIC message switch for the administration of criminal justice.

1.3.7 RETENTION: CHRI which the User maintains, whether retrieved from III or Florida's criminal history record system, shall be kept in a secure records environment to prevent unauthorized access. Retention of CHRI is governed by the record retention schedule for law enforcement published by the Florida Department of State, GS2.

1.3.7.1 Retention of criminal history records, whether retrieved from III or the state system, for extended periods may be appropriate when the time sensitivity of the specific record is important.

1.3.7.2 When, in the sound judgment of the User, retention of criminal history records, whether retrieved from III or the state system, is no longer required, final disposition will be accomplished in a secure manner in compliance with state law, FCIC/NCIC and III rules, regulations and operating procedures to preclude unauthorized access.

1.3.7.3 Because CHRI may become outdated at any time, a current criminal history record check should be performed whenever CHRI is used or relied upon by the User. Entry or retention of criminal history records in a separate or local database would be inconsistent with this principle, and is therefore discouraged. The retention of criminal history records, whether retrieved from III or the state system, in a secondary (non-FDLE) database is not authorized by law.

1.3.8 CRIMINAL HISTORY TRANSMISSION: Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHRI only when an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the public.

1.3.8.1 A facsimile machine may be used to transmit criminal history information between criminal justice agencies, provided both agencies have an NCIC Originating Agency Identifier (ORI) and are authorized to receive

criminal history information. Appropriate measures shall be taken to prevent unauthorized viewing or receipt by unauthorized persons

1.3.9 TRANSACTION LOGGING: Each interface agency accessing FCIC/NCIC and III systems shall ensure that an automated transaction log is maintained. The FCIC/NCIC portion of this log shall be maintained for a minimum of twelve months, and the III portion shall be maintained for a minimum of four years.

1.3.9.1 Automated transaction logging is a feature included in the application software provided by FDLE, and local agencies are encouraged to retain these logs for future reference. Users purchasing or developing an interface to FCIC shall ensure transaction logging is an included feature.

1.3.9.2 The automated transaction log shall identify: the operator on all transactions, the agency authorizing all transactions, the requester and secondary recipient for all criminal history transactions. This information can be captured at log-on and can be a name, badge number, serial number, or other unique identifier.

1.3.9.3 The User may only disseminate CHRI to another authorized recipient and shall maintain a record of any dissemination of state or federal criminal history information. This record shall reflect at a minimum: (1) date of release; (2) to whom the information relates; (3) to whom the information was released; (4) the State Identification (SID) and/or the FBI number(s); (5) the purpose code and (6) the reason for which the information was requested.

1.3.10 INFORMATION ACCESS: The User shall allow only properly screened (as per Section III, paragraph 2 of this User Agreement), authorized personnel performing a criminal justice function who have received proper security awareness training to have access to information contained within the CJNet, FCIC/NCIC or other state or federal criminal justice information system accessed through the FCIC message switch, FBI CJIS Wide Area Network or Internet. The User will also provide assistance to other criminal justice agencies not equipped with direct FCIC access in compliance with FCIC/NCIC and III rules, regulations and operating procedures, but only to the extent that such assistance is not otherwise prohibited.

1.3.10.1 The User shall ensure that all personnel who initiate a transaction to the FCIC message switch are current in CJIS certification.

1.3.10.2 Each individual user shall be properly authenticated prior to initiating a transaction to or requesting information from FCIC or other CJNet application.

1.3.10.3 The User shall ensure that persons allowed to complete CJIS certification are at least 18 years of age and are U.S. citizens or have a valid immigration status/visa.

1.3.10.4 FDLE reserves the right to deny FCIC, CJNet or related programs/ systems access to any individual based on valid, articulable concerns for the security and integrity of FCIC, CJNet or related programs/ systems.

1.3.11 WORKSTATION: FDLE is not responsible for the workstation acquisition, maintenance, operation, repair, supplies or workstation operation personnel costs. The User shall immediately notify the FDLE Customer Support Center, should an FCIC/NCIC workstation or device, associated with an FCIC/NCIC entry(ies), malfunction or become inoperable. All costs associated with returning the workstation to operation, other than CJNet costs, shall be the User's responsibility. FDLE will assist with executing trouble-shooting procedures.

1.4 Interface Operations: For systems implemented after December 31, 2008, the User shall ensure that all automated interfaces that programmatically (i.e., without human intervention) generate transactions to the FCIC message switch are restricted to no more than one transaction per second per interface.

2. AUDITS: The User shall permit an FDLE appointed inspection team to conduct inquiries with regard to any allegations or potential security violations, as well as for routine audits.

2.1 FDLE conducts regularly scheduled compliance and technical security audits of every agency accessing the CJNet to ensure network security, conformity with state law, and compliance with all applicable FDLE, CJNet, FCIC/NCIC and III rules, regulations and operating procedures. Compliance and technical security audits may be conducted at other than regularly scheduled times.

3. TRAINING: The User is responsible for complying with training requirements established in CSP and the rules, regulations, and policies established by FCIC/NCIC, III, FDLE and other CJNet applications. The User is responsible for

remaining current in the applications, procedures, and policies and ensuring personnel attend these training sessions.

3.1 All User personnel who access CJI for the administration of criminal justice shall complete security awareness training, including but not limited to criminal justice officials, e.g., Police Chiefs, Sheriffs, Judges, State Attorneys, etc.

3.2 Only operators who have successfully completed CJIS certification shall be allowed to have unsupervised access to the FCIC/NCIC system.

3.3 FCIC/NCIC operators who are in their initial six months of assignment may be permitted supervised access to FCIC/NCIC. Operators shall successfully complete CJIS certification within six months of appointment or assignment to duties requiring direct access to FCIC/NCIC.

3.4 The User shall require all personnel who are authorized to initiate a transaction to the FCIC message switch to successfully complete CJIS Certification. The User agrees to remove from FCIC/NCIC access any employee who fails to achieve required certification standards, whose certification has expired, whose certification is otherwise rescinded or as directed by FDLE.

3.5 The User shall require all information technology (IT) personnel, including any vendor or contracted staff who will in the course of their contracted criminal justice support duties initiate a transaction to the FCIC message switch, to successfully complete CJIS certification.

3.6 The User shall maintain training records for all personnel with access to CJI, i.e., CJIS certification and security awareness training.

3.7 The User shall require all IT personnel, including any vendor, responsible for maintaining/supporting any IT component used to process, store or transmit any unencrypted CJI, to successfully complete and maintain in current status the CJIS security awareness training provided by FDLE.

4. RELOCATION: Should the User desire to relocate the data circuit(s) and/or equipment connected to CJNet, the User shall provide FDLE written notice 90 days in advance of the projected move. All costs associated with the relocation of the equipment and the data circuit(s), including delays in work order dates, will be borne by the User unless FDLE has funding to make changes without charge. The repair and cost of any damages resulting from such relocation will be the User's responsibility.

4.1 The User shall also provide 90 days advance notice when requesting additional access to FCIC.

5. LIABILITY: The User understands that the FDLE, its officers, and employees shall not be liable in any claim, demand, action, suit, or proceeding, including, but not limited to, any suit in law or in equity, for damages by reason of, or arising out of, any false arrest or imprisonment or for any loss, cost, expense or damages resulting from or arising out of the acts, omissions, or detrimental reliance of the personnel of the User in entering, removing, or relying upon information transmitted through CJNet or in the FCIC/NCIC and NLETS information systems.

6. CRIMINAL HISTORY RECORDS: FDLE is authorized to establish a statewide biometric identification system and an intrastate system for the communication of information relating to crimes, criminals and criminal activity.

   To support the creation and maintenance of the criminal history files, the User, as appropriate, shall:

   6.1 Provide for inclusion in criminal history records information systems, adult and juvenile criminal fingerprints on all felony arrests; adult criminal fingerprints on all misdemeanors and comparable ordinance violation arrests; and juvenile fingerprints on misdemeanor arrests specified at Section 943.051, F.S. The submission of other juvenile misdemeanor arrest fingerprints is optional.

   6.2 Provide security for CHRI and systems that process or store CHRI, and security training for personnel who receive, handle or have access to CHRI.

   6.3 Screen all personnel who will have direct access to CHRI and reject for employment personnel who have violated or appear unwilling or incapable of abiding by the requirements outlined in this agreement.

   6.4 Defer to FDLE on any determination as to what purposes qualify for criminal justice versus non-criminal justice designation, as well as with respect to other purposes that may be authorized by law.

   6.5 As authorized by Florida Statutes and/or federal regulations, the User may share state CHRI. Dissemination of information requires compliance with all applicable statutes, FCIC/NCIC and III rules, regulations and operating procedures, including logging. Agencies shall maintain the restriction on dissemination applicable to such record information, including but not limited to confidentiality or exemption from Section 119.07(1), F.S., as provided by law.

   6.6 Provide security and establish policies to prevent unauthorized access to or dissemination of sealed records, or unauthorized notification of expunged records.

7. As FALCON is a CJI system, the User shall adhere to all policies regarding access, use and dissemination of CHRI. The User shall comply with all training and other appropriate requirements associated with its criminal justice status. The

User shall review FALCON subscriptions to determine whether the User is still authorized to receive criminal history record information on an individual. The User shall indicate the continued authorizing relationship with that individual, i.e., the person is still employed, volunteering, etc., or is currently the subject of investigation or under supervision by the User. CHRI received as a result of a FALCON subscription may be disseminated for criminal justice purposes, and is subject to the same legal and policy restrictions associated with CHRI.

SECTION III SECURITY REQUIREMENTS

1. The User shall comply with the CSP and the rules, regulations, policies and procedures established for CJNet, FCIC/NCIC, III and NLETS, which include but are not limited to System Security, Personnel Security, Physical Security, User Authorization, Technical Security, Dissemination of Information Obtained from the Systems, and Destruction of Records. By accepting access as set forth above, the User agrees to adhere to the following security policies in order to ensure continuation of that access:

2. PERSONNEL BACKGROUND SCREENING: At a minimum, the User shall conduct a state and national fingerprint-based records check on 1) all personnel who are authorized to access state and/or national CJI data or systems, 2) IT personnel who maintain/support information technology components used to process, transmit or store unencrypted CJI, and 3) other personnel, including but not limited to support personnel, contractors and custodial staff, with unescorted physical or logical access to physically secure locations, as defined in the CSP and/or IT components used to process, transmit or store unencrypted CJI. The User is strongly encouraged to screen the applicant by other available means, e.g., local court records, in addition to the fingerprint-based record check.

   2.1 The User shall submit applicant fingerprints of persons described in Section III, paragraph 2, for positive comparison against the state and national criminal history and for searching of the Hot Files.

   2.2 The results of the fingerprint-based record check shall be reviewed prior to granting access to CJI or components used to process/store CJI, including access for IT support. The User may conduct a preliminary on-line criminal justice employment check using Purpose code "J" for this purpose.

      2.2.1 If a record of any kind exists, the User shall consult the FDLE Guidelines for CJIS Access and notify the CSO for review. Upon notification from the User, the CSO shall review the matter to determine if access is appropriate and officially notify the User in writing of the CSO's decision regarding access.

      2.2.2 Once the original background screening has been completed, if the User learns that an employee with access to CJI, including any personnel as identified in Section III, paragraph 2, has a criminal

history or pending charge(s), the User shall consult the FDLE Guidelines for CJIS Access and notify the CSO. The CSO shall review the facts and circumstances and notify the User in writing regarding access to CJI.

2.2.3 The User shall have a written policy for discipline of personnel who 1) access CJNet and/or CJI for purposes that are not authorized, 2) disclose information to unauthorized individuals, or 3) violate FCIC/NCIC or III rules, regulations or operating procedures.

2.3 As the CSA for the State of Florida, the FDLE reserves the right to deny individual user access to any system or related program that is used to process, transmit or store CJI based on valid, articulable concerns for the security and integrity of the information and/or related systems.

2.4 The User shall ensure the appropriate ORI is used for submission of applicant fingerprints. Fingerprints submitted for positions associated with the administration of criminal justice or as required by the CSP, shall include the User's criminal justice ORI. Fingerprints submitted for any other positions not related to the administration of criminal justice or required by the CSP shall include the appropriate and approved non-criminal justice ORI.

3. PHYSICAL SECURITY: The User shall identify facilities, areas, rooms, etc. where CJI is accessed, processed and/or stored to determine physical security requirements as identified in the CSP. The User may designate a facility, area, room, etc., either a physically secure location or a secured area, as defined in the CSP, provided the appropriate requirements are met. Access shall be limited to persons needing access for completion of required duties. The User shall have a written policy that ensures and implements security measures, secures devices that access FCIC/NCIC/CJNet and prevents unauthorized use or viewing of information on these devices. The use of password protected screen blanking software is recommended for devices that access FCIC/NCIC when the operator may leave the computer unsupervised. FDLE reserves the right to object to equipment location, security measures, qualifications and number of personnel who will be accessing FCIC/NCIC and to suspend or withhold service until such matters are corrected to FDLE's reasonable satisfaction.

4. ADMINISTRATIVE SECURITY: The User shall designate individual agency contacts, as described below, to assist the User and FDLE in ensuring compliance with this Agreement. Training for these positions is provided by FDLE, and the User shall ensure that its designee is keenly aware of the duties and responsibilities of each of the following positions. FDLE reserves the right to object to the Users appointment of a TAC, LASO, LAI or AAA based on valid, articulable concerns for the security and integrity of FCIC, CJNet or related programs/systems. The User shall provide FDLE with up-to-date contact information for these positions.

4.1 TERMINAL AGENCY COORDINATOR: The User shall designate a Terminal Agency Coordinator (TAC) to ensure compliance with FCIC/NCIC and III rules, regulations and operating procedures, and to facilitate communication between FDLE and the User. The TAC shall maintain a current CJIS Certification. TACs shall attend TAC training within six (6) months of being assigned to the position, and as often, as required by FDLE, thereafter.

4.2 LOCAL AGENCY SECURITY OFFICER: The User shall designate a Local Agency Security Officer (LASO) to ensure compliance with the CSP. Within six months of assignment to the position, the LASO is encouraged to complete any appropriate LASO training made available by FDLE, including CJIS security awareness training.

4.3 In addition to TAC and LASO, there are other points of contact and positions necessary to manage applications and facilitate communication between the User and FDLE. These positions are identified on the Agency CJIS Contact Form, which may be found on the CJNet CJIS Resource Center website under CJIS Forms and Publications.

5. MANAGEMENT CONTROL AGREEMENTS: In situations where data processing/information services, law enforcement dispatch functions or human resources functions are provided by a non-criminal justice governmental entity, the User shall enter into a management control agreement as required by the CSP. In situations where governmental structure or hierarchy does not support or permit an agreement between the parties involved, a directive which includes all of the provisions for a management control agreement identified in the CSP may be substituted.

6. INTERAGENCY AGREEMENTS: The User shall execute an Interagency Agreement with any other criminal justice agency to which criminal justice information services are outsourced, including but not limited to information technology related functions. The User shall consult with FDLE to determine if a given function requires an Interagency Agreement.

7. TECHNICAL SECURITY

7.1 Remote access services to CJI, including, but not limited to access to FCIC/NCIC and CJNet via the User's Network, will be permitted provided the User establishes appropriate security measures to ensure compliance with all rules, regulations, procedures, and the CSP.

7.2 All FCIC/NCIC/III data transmitted over any public network segment shall be encrypted as required by the CSP. This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is not under the direct security control of a criminal justice agency.

7.3 The User shall maintain, in current status, and provide upon request by FDLE a complete topological drawing, which depicts the User's network configuration as connected to CJNet. As required by the CSP, this documentation shall clearly indicate all network connections, service agencies and interfaces to other information systems.

7.4 The User shall ensure only authorized criminal justice agencies or agencies authorized by FDLE are permitted access to the CJNet via the User's CJNet connection.

7.5 The User shall ensure all devices with connectivity to CJNet employ virus protection, anti-spam and anti-spyware software and such software shall be maintained in accordance with the software vendor's published updates.

7.6 CJI, including but not limited to information obtained from the FCIC message switch and CJNet, may only be accessed via computers or interface devices owned by the User or by the contracted entity. Vendors under contract with the User to perform the administration of criminal justice may be allowed to use their own devices for access provided all requirements of the FBI CJIS Security Addendum are satisfied.

7.7 The User shall ensure that CJNet-only devices have a Windows or network type password to prevent unauthorized access.

7.8 Provided appropriate security precautions are in place, and upon approval from the FDLE Network Administration staff, the User may employ wireless network connectivity (for example the 802.11 wireless networking protocol).

8. COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY: The User shall have a written policy documenting the actions to be taken in response to a possible computer security incident. The policy shall include identifying, reporting, investigating and recovery from computer security incidents. The User shall immediately notify the CSO of any suspected compromise of the CJNet.

9. SECURITY AUTHORITY: All policies, procedures and operating instructions contained in the CSP and FCIC/NCIC, III and NLETS documents, operating manuals and technical memoranda, are hereby incorporated into and made a part of this agreement, except to the extent that they are inconsistent herewith or legally superseded by higher authority.

10. CLIENT SOFTWARE LICENSE: The FCIC Client Software (eAgent) license from Diverse Computing, Incorporated is located in the Help menu of the eAgent client software. The FCIC Client Software (eAgent) license is made a part of and incorporated by reference into this User Agreement and shall be binding on the User upon acceptance of the software. The User is allowed up to one hundred (100) eAgent Subswitch mnemonics. The User is not permitted to install eAgent, as provided by FDLE, on laptops for use in a mobile environment, including tablets, netbooks and other "handheld" devices. The User is not permitted to use the eAgent client software as an interface to the FCIC message switch for another application.

11. PRIVATE VENDORS: Private vendors which, under contract with the User, are permitted access to information systems that process CJI, shall abide by all aspects of the FBI CJIS Security Addendum.

    11.1 The contract between the User and the vendor shall incorporate the FBI CJIS Security Addendum to ensure adequate security of CJI.

    11.2 The User shall ensure all vendor employees are appropriately screened prior to granting the vendor employees access to CJI. Vendor employee fingerprints submitted by the User to FDLE as required by the CSP shall be taken/rolled/printed by a recognized law enforcement agency or an FDLE approved third party vendor. NOTE: A vendor may not fingerprint its own employees.

    11.3 The User shall maintain the Security Addendum Certification form for each member of the vendor staff with access to information systems that processes CJI.

    11.4 The User shall ensure all vendor employees with access to CJI have received the appropriate security awareness training via the CJIS Online application and are in current status.

    11.5 The User shall ensure private vendors permitted such access are aware of the provisions of Section 817.5681, F.S. regarding breach of security of personal information.

    11.6 The User shall contact FDLE for review prior to entering into a contract or agreement with a private vendor in the course of which state or national CJI is processed, stored or transferred from the User's physically secure location to a vendor owned or operated facility(s) (e.g., cloud services.)

    11.7 The User shall maintain and keep current a list of all vendor employees who have been authorized access to CJI.

12. USERNAMES and PASSWORDS/AUTHENTICATION: The User shall ensure that all personnel, including IT support and vendors, who initiate a transaction to the FCIC message switch have a separate and distinct username and password/ authentication for the software/interface used to initiate the transaction.

    12.1 The User shall ensure that all User-operated interfaces, including but not limited to computer aided dispatch systems, record management systems, jail management systems and mobile data systems with the FCIC message switch or other systems that contain CJI, follow the password requirements as outlined in the CSP.

    12.2 Individual users shall refrain from sharing passwords and/or other authenticators, including but not limited to smart cards, tokens, public key

infrastructure (PKI) certificates, etc., used to access CJI or CJNet related systems.

12.3 Individual users shall refrain from using another individual's account or session for the purpose of accessing CJI or other CJNet applications.

12.4 Individual users shall refrain from caching credentials/passwords for access to systems/applications used to process or store CJI.

12.5 All personnel with access to any system or application that processes or stores CJI for maintenance or administration purposes shall be uniquely identified.

13. INDIVIDUAL USER ACCESS: The User shall deactivate individual user access to eAgent and/or other FCIC interfaces, other CJNet applications and other state/federal systems containing CJI, including but not limited to LEO and/or NDEx, upon separation, reassignment or termination of duties, provided individual user access is no longer required for the administration of criminal justice.

14. OFF SITE STORAGE/PROCESSING OF CJI: The User shall contact and receive approval from the CSO prior to entering into an agreement with a noncriminal justice governmental agency for off-site storage or processing of CJI (often referred to as cloud computing or cloud services.)

SECTION IV MISCELLANEOUS REQUIREMENTS

1. FDLE has received funding from the United States Department of Justice and is subject to and must demand intrastate users of its criminal history record services adhere to US Code (28 U.S.C. section 534), State Statute (Chapter 943 F.S.), Code of Federal Regulations (28 C.F.R. Part 20), Florida Administrative Code (Chapter 11C-6, F.A.C.), FCIC/NCIC and III rules, regulations and operating procedures which this agreement incorporates both present and future.

2. PENALTIES AND LIABILITIES: Any non-compliance with the terms of this Agreement concerning the use and dissemination of criminal history information may subject the User's officers or employees to a fine not to exceed $11,000 as provided for in the Code of Federal Regulations, Title 28, Section 20.25, and/or discontinuance of service. Moreover, certain offenses against system security and the information contained therein are crimes under Florida Statutes and can result in criminal prosecution.

3. PROVISIONS INCORPORATED: The User shall be bound by applicable federal and state laws, federal regulations and the rules of FDLE to the same extent that the User would be if such provisions were fully set out herein. Moreover, this Agreement incorporates both present and future law, regulations and rules.

4. TERMINATION: Either party may terminate this Agreement, with or without cause, upon providing advanced written notice of 45 days. Termination for cause includes, but is not limited to, any change in the law that affects either party's ability to substantially perform as provided in this Agreement. Should the aforementioned circumstances arise, either party may terminate or ask to modify the Agreement accordingly.

    4.1 FDLE reserves the right to terminate service, without notice, upon presentation of reasonable and credible evidence that the User is violating this Agreement or any pertinent federal or state law, regulation or rule.

5. MODIFICATIONS: Modifications to the provisions in this Agreement shall be valid only through execution of a formal written amendment.

6. ACCOUNTABILITY: To the extent provided by the laws of Florida, and without waiving any defenses or immunities to which the User may be entitled, the User agrees to be responsible for the negligent acts or omissions of its personnel arising out of or involving any information contained in, received from, entered into or through CJNet, FCIC/NCIC, III and NLETS.

7. ACKNOWLEDGEMENT: The User hereby acknowledges the duties and responsibilities as set out in this Agreement. The User acknowledges that these duties and responsibilities have been developed and approved by FDLE to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the CJNet, including the FCIC/NCIC System. The User further acknowledges that failure to comply with these duties and responsibilities may subject its access to various sanctions as approved by the FBI Criminal Justice Information Services Advisory Policy Board. These sanctions may include termination of NCIC services to the User. The User may appeal these sanctions through the CSA.

8. TERM OF AGREEMENT: This agreement will remain in force until it is determined by FDLE that a new agreement is required. The User should initiate the execution of a new agreement when a change of agency chief executive or official occurs.

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

NAME OF THE USER AGENCY Orlando Police Department

USER CHIEF EXECUTIVE or OFFICIAL

John W. Mina **TITLE** Chief of Police
(PLEASE PRINT)

(SIGNATURE)

DATE

WITNESS **TITLE**

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY Donna M. Uzzell **TITLE** CJIS Director
(PLEASE PRINT)

(SIGNATURE)

DATE

WITNESS **TITLE**