DEPARTMENT OF FINANCIAL SERVICES
Data Security Requirements

Addendum B

1. **Data Security, Recovery, and Damages for Non-Performance**.

a. Data Security. The Contractor, its employees, subcontractors, and agents, shall comply with Rule Chapter 60GG-2, Florida Administrative Code (F.A.C.), which contains information technology (IT) procedures and requires adherence to the Department's security policies, in performance of this Contract. The Contractor shall provide immediate notice to the Department's Information Security Office (ISO), within the Office of Information Technology: 1) in the event it becomes aware of any security breach or any unauthorized transmission or loss of any or all of the data collected, created for, or provided by the Department (State Data); and 2) of any allegation or suspected violation of Rule Chapter 60GG-2, F.A.C. Except as required by law or legal process, and after notice to the Department, the Contractor shall not divulge to third parties any Confidential Information obtained by the Contractor or its agents, distributors, resellers, subcontractors, officers, or employees in the course of performing Contract work according to applicable rules, including, but not limited to, Rule Chapter 60GG-2, F.A.C. "Confidential Information" means information in the possession or under the control of the state of Florida (State) or the Contractor that is exempt from public disclosure pursuant to chapter 119, Florida Statutes (F.S.), or to any other applicable provision of State or federal law that serves to exempt information from public disclosure. This includes, but is not limited to, the security procedures, business operations information, or commercial proprietary information in the possession of the State or the Department. The Contractor will not be required to keep confidential any information that is publicly available through no fault of the Contractor, material that the Contractor developed independently without relying on the State's Confidential Information, or information that is otherwise obtainable under State law as a public record. If State Data will reside in the Contractor's system, the Department may conduct, or request the Contractor conduct at the Contractor's expense, an annual network penetration test or security audit of the Contractor's system(s) on which State Data resides. If the Contract is less than a year in duration, the right to conduct the network penetration test or security audit of the Contractor's system(s) on which State Data resides can be exercised at any time.

b. Data Protection. No State Data will be transmitted, processed, or stored outside of the United States of America regardless of method, except as required by law. Access to State Data will only be available to staff approved and authorized by the Department that have a legitimate business need. Access to State Data does not include remote support sessions for devices that might contain the State Data; however, during the remote support session the Department requires the Contractor to escort the remote support access and maintain visibility of the support personnel's actions. Requests for remote access will be submitted to the Department's Help Desk. With approval, third parties may be granted time-limited terminal service access to IT resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools. When remote access is no longer needed, the ISO will be promptly notified and access will be promptly removed.

c. Encryption and Remote Access. The Contractor shall encrypt all data transmissions containing Confidential Information utilizing a protocol approved by the Department.

d. Breach and Negligence. The Contractor agrees to protect, indemnify, defend, and hold harmless the Department from and against any and all costs, claims, demands, damages, losses, and liabilities arising from or in any way related to the Contractor's breach of this Section 1 or the negligent acts or omissions of the Contractor related to this addendum.

e. Separate Security Requirements. Any Criminal Justice Information Services-specific and/or Health Information Portability and Accountability Act-specific security requirements are attached in a separate addendum, if applicable.

f. Ownership of State Data. State Data will be made available to the Department upon its request, in the form and format reasonably requested by the Department. Title to all State Data will remain property of the Department and/or become property of the Department upon receipt and acceptance. The Contractor shall not possess or assert any lien or other right against or to any State Data in any circumstances.

2. Data Access.

a. Background Checks. All Contractor personnel who will have direct query access to State Data will undergo background checks as follows:
The Contractor's staff provided to perform the work described in Attachment 2, Statement of Work, must undergo a background check at the expense of the Contractor. Review and approval of a background check, which, at a minimum, is the equivalent of a Level 2 Criminal Background Screening described in section 435.04, F.S., including fingerprinting, is required for the Contractor's staff before he or she will be allowed to perform work under the Contract. The Contractor must advise the Contractor's staff that: (i) the fingerprints will be used to check the criminal history records of the FBI (depending on the SOW scope, the fingerprints may be used on an ongoing basis to check the criminal history records of the FBI, which may include expunged records), and (ii) procedures for obtaining a change, correction, or update of an FBI identification record are described in 28 C.F.R. 16.34. Results will be used to determine the Contractor's staff eligibility for access to the Department's systems. The Department will provide detailed instructions for fingerprinting upon selection.

b. Cooperation with the State and Third Parties. The Contractor agrees to cooperate with the following entities: (i) the State; (ii) the State's other contractors; (iii) the State's agents, including properly authorized governmental entities; (iv) the State's authorized third parties, such as technology staff under contract with the State; and (v) other properly authorized individuals who directly or indirectly access State Data on behalf of any of the entities listed in this section. The Contractor shall also provide reasonable access to the Contractor's Contract personnel, systems, and facilities to these same entities, when reasonably requested by the Department. The Contractor agrees to impose these same requirements on all subcontractors performing the work of this Contract.