DEPARTMENT OF FINANCIAL SERVICES

Data Security Requirements

Addendum B

1. **Data Security.**
The Contractor, its employees, subcontractors, and agents, shall comply with Rule Chapter 74-2, Florida Administrative Code (F.A.C.), which contains information technology (IT) security procedures and requires adherence to the Department's security policies, the relevant parts of which are contained herein, in performance of this Contract. The Contractor shall provide immediate notice to the Department's Information Security Office, within the Office of Information Technology, 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). 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 74-2, F.A.C. "Confidential Information" means information in the possession of, 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.

2. **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 remote support sessions the Department requires the Contractor to escort the remote support access and maintain visibility of the support personnel's actions. The Contractor shall encrypt all data transmissions containing Confidential Information. 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 addendum or the negligent acts or omissions of the Contractor related to this addendum.

3. **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. The Contractor shall develop data security procedures to ensure only authorized access to data submissions by personnel for contracted activities.

4. **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.