DEPARTMENT OF FINANCIAL SERVICES
Data Security Requirements

Addendum B

1. Definitions.

For the purposes of this Addendum, the following terms are defined as set forth below:

a. Cloud Computing – A service, solution, or option as defined in 60GG-4.001, F.A.C.
b. Cloud Service Provider – Person, organization, or entity responsible for making a cloud computing service, solution, or option available to a consumer.
c. Contractor – The entity selected to provide goods or services to the Department and its employees, officers, subcontractors, agents, representatives, distributors, and resellers.
d. Data-at-Rest – Stationary electronic or digital Open Data and Non-Open Data stored in any digital form or medium.
e. Department – The Department of Financial Services, an agency of the State.
f. Breach – A confirmed event that compromises the confidentiality, integrity, or availability of information or data.
g. Non-Open Data – Any data that is in the possession or under the control of the State or the Contractor that is confidential information exempt from public disclosure pursuant to chapter 119, Florida Statutes, (F.S.); personal information enumerated in section 501.171(1)(g), F.S.; and/or any data that is restricted from public disclosure based on federal or state laws and regulations, including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws. Non-Open Data also includes data that any state agency, the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services is statutorily authorized to assess a fee for its distribution.
h. Open Data – Any and all data meeting the definition of "Open data" in section 282.0041, F.S.
i. State – The state of Florida.

2. Data Security.

a. The Contractor shall meet or exceed the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, as detailed in Rule Chapter 60GG-2, Florida Administrative Code (F.A.C.).
b. The Contractor shall comply with section 501.171, F.S., to protect and secure Non-Open Data.
c. The Contractor shall provide notice to the Department within twenty-four (24) hours of confirmation that a Breach of Non-Open Data has occurred or within twenty-four (24) hours of the Contractor having a reasonable belief that a Breach of Non-Open Data has occurred. Notice must be provided to the Department's Security Operations, Office of Information Technology, via email to DFS-SecurityOpsAlerts@myfloridacfo.com or via telephone at (850) 413-2231.
d. If Non-Open Data will reside in the Contractor's system, the Department may require the Contractor to conduct, at the Contractor's expense, an annual network penetration test or security audit of the Contractor's system(s) on which any Non-Open Data resides (test/audit). But such tests/audits need not duplicate those conducted by the Contractor for other purposes if said tests/audits fulfill the Department's requirements. If this Contract duration is less than one year, the Department's right to require that the Contractor conduct said tests/audits can be exercised at any time. If the Contractor conducts the test/audit, then the Contractor shall prepare an assessment report and submit it to the Department for its review. Each assessment report shall contain, at a minimum, any exceptions or deficiencies and whether those exceptions or deficiencies are correctable. The Contractor shall ensure

the Department's Contract Manager's receipt of the assessment report that resulted from the test/audit in Adobe Acrobat PDF (.pdf) format, within ten (10) Business Days of the Contractor's completion of the report, or within ten (10 days after the Department's request of the report (if the test/audit had been conducted within the prior twelve (12) months on the Contractor's system(s) on which any of the Department's Non-Open Data resides). If any said test/audit detects any exceptions or deficiencies, the Contractor shall cooperate with the Department by responding to and promptly correcting the correctable items.

e. If the Contractor is a Cloud Service Provider, the Contractor shall engage a certified public accounting firm on an annual basis, and at no additional cost to the Department, to perform a Statement on Standards for Attestation Engagements SSAE 18 SOC 2 Type II audit in accordance with the professional standards established by the American Institute of Certified Public Accountants (AICPA) for all systems used to comply with data security obligations under this Contract. The Contractor shall ensure the Department's Contract Manager's receipt of the annual audit report in Adobe Acrobat PDF (.pdf) format, within ten (10) Business Days of the Contractor's receipt of the report from the auditor. The Department's expectation is that all audits conducted will find the Contractor in full compliance with all data security standards. If an auditor notes any exceptions or deficiencies the Contractor shall provide its audit response and identify any correctable items to the Department.

3. Disclosure Restrictions.

The Contractor shall not divulge to any third party any Non-Open Data obtained by the Contractor in the course of performing its contracted work unless required by law or legal process, and only after notice to 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 Non-Open Data, or information that is otherwise obtainable under State law as a public record.

4. Data Access and Storage.

a. No Data-at-Rest will be stored outside of the continental United States of America regardless of method or medium, except as required by law or approved in writing by the Chief Financial Officer (CFO) or the CFO's designee.

b. Access to Non-Open Data will only be available to personnel with a legitimate business need who are approved and authorized by the Department.

c. Requests for remote access shall be submitted to the Department's Contract Manager. With approval from the Department, third parties may be granted time-limited terminal service access to IT resources as necessary for the 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 Contractor shall notify the Department's Contract Manager, and access shall be promptly removed.

d. Remote access to data other than Open Data from outside of the continental United States is prohibited unless approved in writing by the CFO or the CFO's designee.

e. If required by the Department, the Department will escort any remote support access and maintain visibility of the Contractor actions during remote support sessions.

5. Offshore Storage of Data.

If a legitimate business need exists that requires the storage of Data-at-Rest outside the continental United States of America, the Contractor may submit a request in writing to allow data to be stored offshore. If such a request is approved, it shall be in writing and signed by the CFO or the CFO's designee. Any such approval will be incorporated into the Contract as Exhibit 1 to this Addendum B, and the Contractor must

comply with any additional restriction contained therein. The Department may rescind its approval for data storage outside of the continental United States of America at any time, if:

a. The Contractor has not complied with terms of Exhibit 1 to Addendum B;
b. The Contractor has not complied with any provision stated in this Addendum B; or
c. The CFO or the CFO's designee determines rescission is in the best interest of the State.

6. Data Encryption and Protection.

The Contractor shall encrypt all data transmissions containing Non-Open Data.

7. Breach and Liability.

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 B or Exhibit 1 to this Addendum B (when applicable) or the negligent acts or omissions of the Contractor related to this Addendum B or Exhibit 1 to this Addendum B (when applicable).

8. 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.

9. Ownership of Non-Open Data.

Non-Open Data shall be made available to the Department upon its request, in the form and format reasonably requested by the Department. Title to all Non-Open 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 Non-Open Data in any circumstances.

10. Cooperation with the State and Third Parties.

The Contractor agrees to cooperate with the following entities: the State, the State's other contractors, the State's agents including properly authorized governmental entities, the State's authorized third parties such as technology staff under contract with the State, and other properly authorized individuals who directly or indirectly access Non-Open 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 providing services under this Contract.