APPENDIX C

INFORMATION SECURITY & CYBER SECURITY REQUIREMENTS

1. Definitions

The term "Confidential Information" as used herein includes all electronic or hard copy information, records, and communications that Contractor has gained or will gain access to in the course of rendering services under this Contract, including, but not limited to, any information, records, or communications that the Department or the State of New York ("State"), regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., the Department, other State agencies, regulated entities, electronic systems, federal government, or third-party Contractors) provides to the Contractor, its officers, agents, employees, and subcontractors or that Contractor, its officers, agents, employees, and subcontractors obtain, discover, derive, or otherwise become aware of as a result of Contractor's performance of services under this Contract. Contractor shall maintain the security, confidentiality, integrity, and availability of all Confidential Information in accordance with the following clauses in the performance of its activities under the Contract. Contractor shall ensure that its officers, agents, employees, partners, and subcontractors, if any, are fully aware of the obligations arising under this Contract and shall take all commercially reasonable steps to ensure their compliance to prevent unauthorized use, access, or disclosure of Confidential Information. Failure by Contractor or its officers, agents, employees, partners, and subcontractors to fully comply with these requirements shall be deemed a failure to meet Contractor's obligations under this Contract and may result in the Department suspending, canceling, and/or terminating the Contract for cause or pursuing any other legal or equitable remedies available.

2. Data and Cyber Security During Contract Term

(a) Compliance with Department and State Information Security Policies and Standards

Contractor warrants, covenants, and represents that it will comply fully with all security policies and standards of the Department in the performance of this Contract, including State Information Technology Services ("ITS") cyber security information security policies and standards located at https://its.ny.gov/policies.

Except for any privilege or privacy right recognized by law, individuals have no legitimate expectation of privacy during any access of the Confidential Information. Any access may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems) and other electronic records. Unauthorized access to Confidential Information is not permitted.

The Department shall have the right at any time to require that Contractor remove from interaction with the Department any Contractor representative whom the Department believes is detrimental to its working relationship with Contractor. The Department will provide Contractor with notice of its determination and the reasons it requests the removal. If the Department signifies that a potential security violation exists with respect to the request, Contractor shall immediately remove such individual. Contractor shall not assign the individual to any aspect of the Contract or future work orders without the Department's consent.

Contractor, to the extent the following meets or exceeds the ITS information security policies described above, shall use industry standard security measures, including standard encryption protocols, to protect and guard the confidentiality, security, integrity, and availability of information, and adhere to all the Department's security policies. Contractor is strictly prohibited from using Confidential Information in any fashion other than that defined herein. There may be instances in which the Department will communicate security procedures necessitated by the Department's operations. Contractor will use reasonable efforts to implement such procedures.

Contractor warrants that it will be properly informed and trained regarding security standards and is prohibited from disclosing Confidential Information to any persons without a need to know.

(b) **Protection and Transmission of Confidential Information**

Contractor shall use appropriate means to preserve and protect Confidential Information. This includes, but is not limited to, preventing the tampering with, disengaging, or otherwise circumventing Department or third-party IT security controls; use of stable storage media; regular data backups and archiving; password protection of volumes; and data encryption. Consistent with the State Encryption Standard found at https://its.ny.gov/policies, to the extent that doing so is applicable based on the specific services provided by Contractor to the Department under this Contract, the Contractor must encrypt Confidential Information at rest, on file storage, database storage, or on back-up media, and in transit in accordance with local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines. Contractor must use up-to-date, secure means for all electronic transmission or exchange of system, user, and application data with the Department, with encryption at rest specifically using, at minimum, FIPS 140-3, Security Requirements for Cryptographic Modules | CSRC (nist.gov), and the secure means used for electronic transmission or exchange of system, user, and application data with the Department shall be up-to-date and align with industry best practices. Contractor agrees that to the extent it has been authorized to use such storage, any and all Confidential Information will only be stored, processed, and maintained on designated devices, and that no Confidential Information at any time will be processed on or transferred to any unauthorized portable computing device or any portable storage medium.

Contractor shall also comply fully with all requirements of this Contract specific to the services Contractor is providing under this Contract. In addition to the specific security provisions required herein, Contractor shall also use, to the extent the following meets or exceeds the Department and the ITS information security policies referenced above, commercially reasonable best efforts to address and remediate any vulnerabilities associated with the types of application development or configuration services it is providing under this Contract. If any system or application security scanning undertaken hereunder reveals vulnerabilities or any other security risks attendant to a provided solution, Contractor is responsible for ensuring those vulnerabilities and risks are remediated in a timely fashion and to the Department's reasonable satisfaction.

(c) **Physical Transport of Confidential Information**

To the extent the Department agrees under this Contract that Contractor may physically transport any Confidential Information, such physical transport may only occur upon the written direction and approval of the Department. This includes but is not limited to transport between the Contractor's offices, to and from third parties, and to and from the Department.

(d) **Data Storage, Access, and Location - Offshore Restrictions**

Contractor may conduct help desk, support services, and software development and testing activities under this Contract from any location convenient to Contractor, except that the Department and Contractor agree that: (a) all Confidential Information shall remain within, and may not be stored or accessed from outside of, the Continental United States ("CONUS"); and (b) unless expressly agreed to in a writing approved by a Department-authorized signatory adhering to established Department practices, Contractor shall not have remote access to the Department's information technology resources.

All access to Confidential Information, physical or virtual, must be conducted within CONUS and have adequate security systems in place to protect against the unauthorized access to State facilities and Confidential Information stored therein. The Contractor shall not send or permit to be sent to any location outside of the CONUS any Confidential Information.

To the extent support by Contractor requires replication of a set of conditions such as a software crash event, Contractor shall replicate that set of conditions in its own environment when providing support, and while communicating with Department technical personnel. For software development activities, such as patches, updates, or adding new functionality, Contractor shall conduct that software development within its own development, quality assurance, and production environments, and, when the software is ready, shall package and provide it through an agreed-to Internet-based location, from which Department technical personnel will download such software, and install and test it in the Department's information technology environment.

Upon the Department's prior written approval, to the extent Contractor requires access to Department system or application audit logs for support and troubleshooting, Contractor or any subcontractors shall maintain such logs only within CONUS, shall take the strictest measures to ensure such logs do not contain Confidential Information including production data, and shall maintain such logs in a secure environment subject to audits by the Department.

(e) **Separation of Duties/Access Controls**

The Contractor must ensure that all Confidential Information that it holds under this Contract is stored in a controlled access environment to ensure data confidentiality, integrity, and availability. Contractor shall provide the Department with a list of the physical locations where Contractor has stored any Confidential Information at any given time and shall update that list if the physical location changes. All Contractor facilities must have adequate security systems in place to protect against the unauthorized access to such facilities and data stored therein. Contractor shall restrict access to and within such facilities through an access control system that requires positive identification of authorized individuals and shall maintain a log of all access (e.g., date and time of the event, type of event, user identity, component of the information system, and outcome of the event). The Contractor shall have a formal procedure in place for granting and terminating computer system access to Confidential Information and to track access. Contractor access to Confidential Information for any types of projects outside of those approved by the Department is prohibited.

The Department requires the Contractor to follow the principle of least privilege by adhering to separation of job duties and limiting Contractor staff knowledge of Confidential Information provided under this Contract to that that is absolutely needed to perform job duties. Upon request, Contractor will provide documentation to the Department clearly defining the security roles and access levels for each of its staff working with Confidential Information provided under this Contract with a level of specificity objectively reasonable to and approved by the Department.

(f) **Cloud Security Requirements**

If cloud-based services are a component of the solution or services to be provided by Contractor, Contractor shall comply with FedRAMP (https://www.fedramp.gov) standards for cloud services, and local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines.

(g) **Compliance with State Statutory Breach Notification and Data Security Requirements**

Contractor shall be responsible for complying with the statutory breach notification and data security requirements set forth in New York General Business Law ("GBL") §§ 899-aa and 899-bb and New York State Technology Law ("State Technology Law") §208 as well as the following terms contained herein with respect to any private information (as

defined in GBL §899-aa) received by Contractor under this Contract ("Private Information") that is within the control of the Contractor either on the Department's information security systems or the Contractor's information security systems. In the event of a breach of the security of the system (as defined by GBL §899-aa), Contractor shall immediately commence an investigation, in cooperation with the Department, to determine the scope of the breach and restore the security of the system to prevent any further breaches. Contractor shall also notify the Department of any breach of the security of the system or any potential breach of the system within four (4) hours following discovery of such breach or potential breach. Notice of such breach or potential breach shall be sent to the Department at:

information.security@dfs.ny.gov

Except as otherwise instructed by the Department, Contractor shall, to the fullest extent possible, first consult with and receive authorization from the Department prior to notifying any individuals, the State Department of State, the State Division of State Police, the State Office of the Attorney General ("OAG"), or any consumer reporting agencies of a breach of the security of the system or concerning any determination to delay notification due to law enforcement investigations.

Nothing herein shall in any way impair the authority of OAG to bring an action against Contractor to enforce the provisions of applicable statutory breach notification and data security provisions or limit Contractor's liability for any violations of GBL §899-aa, GBL §899-bb, State Technology Law §208, or any other applicable laws, rules, or regulations. In the event that the Contractor is advised by a law enforcement agency pursuant to GBL §899-aa(4) to delay the notice under GBL §899-aa(3), the Contractor shall provide the notice to the Department not more than twenty-four (24) hours after the Contractor has been advised that it may provide the notice under GBL §899-aa(3).

In accordance with applicable statutory breach notification and data security provisions, Contractor is responsible for complying with the following terms with respect to any Private Information received by or on behalf of the Department under this Contract. The Contractor:

(i) Shall supply the Department with a copy of its breach notification policy, which shall be modified to be in compliance with this Appendix.
(ii) Shall encrypt any database fields and backup tapes that contain Private Information as set forth in applicable statutory breach notification and data security provisions.
(iii) Shall ensure that the Private Information is encrypted in transit to/from Contractor's systems.
(iv) Shall ensure that Private Information is not displayed to users on computer screens or in printed reports; however, specific users who are authorized to view the private data elements and who have been properly authenticated may view/receive such data.
(v) Shall monitor for breaches of security to any of its systems that store or process

Private Information.

(vi) Shall take all steps as set forth in applicable statutory breach notification and data security provisions to ensure that Private Information will not be released without authorization from the Department.

(vii) In the event a security breach occurs as defined by GBL §899-aa, shall notify the Department's contact at information.security@dfs.ny.gov within four (4) hours of becoming aware of the breach and commence an investigation in cooperation with the Department to determine the scope and cause of the breach, and to prevent the future recurrence of such security breaches.

(viii) Shall coordinate all communication regarding the data breach with the Department's Chief Information Security Officer.

(ix) Shall take immediate steps necessary to restore the information security system to prevent further breaches and take corrective action in the timeframe required by the Department and State. If Contractor is unable to complete the corrective action within the required timeframe, in addition to any other remedies available, the Department and/or the State may contract with a third-party to provide the required services until corrective actions and services resume in a manner acceptable to the Department, or until the Department has completed a new procurement for a replacement service system. The Contractor will be responsible for the cost of these services during this period.

(x) Shall be responsible for providing all notices required by applicable statutory breach notification and data security provisions and for all costs associated with providing said notices.

The Department reserves the right to require commercially standard credit monitoring for any and all individuals affected by any data breach at the sole expense of the Contractor for a period to be determined by the Department, but not less than twelve (12) months, which shall begin thirty (30) days following the notice of offer from the Contractor of such credit monitoring to those affected individuals, which shall be within a reasonable time following the identification of such affected individuals. The Department reserves the right to require notice by regular or electronic mail.

(h) **Breaches Not Addressed by GBL §899-aa, GBL §899-bb, or State Technology Law §208**

In addition to any responsibilities of Contractor under the Contract for reporting breaches of Private Information under GBL §899-aa, GBL §899-bb, or State Technology Law §208, Contractor must, within four (4) hours of becoming aware of a breach, report to the Department *any* breaches or information security incidents of any Confidential Information whether it consists of Private Information or otherwise. Notice of such incident shall be sent to the Department at:

information.security@dfs.ny.gov

Contractor shall ensure that the personnel charged with carrying out services under this Contract are aware of Contractor's obligations to the Department hereunder.

Contractor's staff's browsing, viewing, altering, appending, or modifying the Confidential Information in violation of Contractor's own security policies shall be deemed to have breached the security of the system for the purposes of this Contract. Contractor represents and warrants that the Confidential Information that it hosts for the Department remains at all times the property of the Department and must be fully accessible to the Department during the term of the Contract and at the Contract's conclusion. Contractor will take all reasonable measures at no additional cost to the Department to ensure that the Department is able to extract or receive any and all Confidential Information out of Contractor's hosted solution, including metadata and attachments, in a format that is reasonably accessible to the Department and capable of being used in technical solutions that compete with Contractor's hosted solution, as further described below.

3. Data Transparency, Accessibility, Migration, and Destruction at End of Contract

(a) **Data Migration**

Contractor shall ensure that the services it performs and the solutions it designs under this Contract are performed in such a way as to ensure easy migration of any Confidential Information held by Contractor as required by the Department. This may include:

(i) Contractor keeping Confidential Information, including Department policy and profile information, separate from processes of any software itself and maintaining that information in a format that allows the Department to easily transfer it to an alternative application platform;

(ii) Contractor making its Application Programming Interfaces (APIs) available to the Department; and

(iii) Contractor reformatting data and/or applications at Contractor's own expense in order to allow the Department easily to switch to alternative software providers or move the Confidential Information back in-house at the Department.

(b) **Data Return and Destruction - In General**

During any period of suspension of services or of the Contract, the Contractor will not take any action intentionally to erase any Confidential Information.

At the expiration or termination of the Contract, the Contractor shall implement an orderly return of Department assets and the subsequent secure disposal of Department assets. The Department shall be entitled to any post-termination assistance generally made available by Contractor with respect to the services it provides unless a unique alternative data retrieval arrangement has been established between the parties.

At the Department's option, the Contractor must provide the Department with a copy of all Confidential Information, including metadata and attachments, in a mutually agreed upon, commercially standard format at no additional charge to the Department, and give the Department continued access to the Confidential Information for no less than ninety (90) days beyond the expiration or termination of the Contract. Thereafter, except for data required to be maintained by local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines or this Contract, Contractor shall destroy Confidential Information from its systems and wipe all its data storage devices to eliminate any and all Confidential Information from Contractor's systems. The sanitization process must be in compliance with State Security Policy NYS-S13-003, located at https://its.ny.gov/policies, and, where required, Criminal Justice Information Services sanitization and disposal standards. If immediate purging of all data storage components is not possible, the Contractor will certify that any Confidential Information remaining in any storage component will be safeguarded to prevent unauthorized disclosures until such purging is possible. Contractor must then certify to the Department, in writing, that it has complied with the provisions of this paragraph including any supporting documentation as requested.

(c) **Data Return and Destruction - Regulated Data**

The Department considers the protection of sensitive and Confidential Information and business systems to be of the utmost importance. The Confidential Information collected and maintained by the Department is protected by a myriad of federal, state, and local laws, rules, regulations, ordinances, policies, standards, and guidelines. Access to and use of Confidential Information is limited to authorized government employees and legally designated agents, for authorized purposes only.

Appendix D to this Contract, entitled "PRIMARY SECURITY AND PRIVACY MANDATES," reflects several significant federal and State laws, rules, regulations, ordinances, policies, standards, and guidelines that providers doing business with the Department must be aware of and comply with if applicable to the services being provided. Links to further guidance are included in that Exhibit. The list is intentionally US-centric and is not intended to be all-inclusive. Further, since local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines and industry guidelines change, consulting definitive sources to assure a clear understanding of compliance requirements is critical.

To the extent that Contractor has access to federal, state, or local government regulated data pursuant to its responsibilities under the Contract, Contractor agrees that it will abide by the requirements of those federal, state, and local laws, rules, regulations, ordinances, policies, standards, and guidelines, and will require in writing its officers, agents, employees, partners or subcontractors to similarly abide by any such requirements including the execution of any documents or contracts required to be executed, certifying their compliance with same.

Contractor must, in accordance with applicable law and the instructions of the Department: maintain such regulated data for the time period required by applicable laws, rules, regulations, ordinances, policies, standards, and guidelines; exercise due care for the protection of data; and maintain appropriate data integrity safeguards against the deletion or alteration of such data. In the event that any regulated data is lost or destroyed because of any act or omission of the Contractor or any non-compliance with the obligations of this Contract, then Contractor shall, at its own expense, use its best efforts in accordance with industry standards to reconstruct such data as soon as feasible. In such event, Contractor shall reimburse the Department for any costs incurred by the Department in correcting, recreating, restoring, or reprocessing such data or in assisting therewith.

In the event that it becomes necessary for Contractor to receive Confidential Information that federal, state, or local laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure, Contractor hereby agrees to return or destroy all such Confidential Information that has been received under this Contract when the purpose that necessitated its receipt by Contractor has been completed. In addition, Contractor agrees, after termination of the Contract, not to retain any Confidential Information that federal, state, or local laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure.

Notwithstanding the foregoing, if the return or destruction of the Confidential Information is not feasible, Contractor agrees to extend the protections of the Contract for as long as necessary to protect the Confidential Information and to limit any further use or disclosure of that Confidential Information. If Contractor elects to destroy Confidential Information, it shall use reasonable efforts to achieve the same and notify the Department accordingly. Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of Confidential Information that federal, state, or local laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure.

4. Audits and Access to State Facilities

(a) Audits of Contractor's Security Controls

Contractor may be asked to provide recent independent audit reports on its security and compliance controls before and during the term of this Contract. The Department shall have the right to send its officers and employees into the offices of the Contractor for inspection and audit of the facilities and operations used by Contractor in the performance of any work under this Contract. On the basis of such inspection, Contractor may be required by the Department to implement specific additional security and compliance measures in cases where the Contractor is found to be non-compliant with Contract safeguards. The Department will provide at least two (2) weeks' notice of its intention to exercise this audit right and will not use an independent third-party that is a competitor of Contractor. Such audit shall be conducted to ensure compliance with the requirements of the Contract.

(b) Accessing State Facilities

Contractor may access Department information technology resources and state facilities solely at the Department's request, and solely for work associated with this Contract. In the event Contractor accesses state facilities, Contractor will comply fully with all security procedures of the Department concerning such access communicated to it in the performance of this Contract or any amendments hereof.

Contractor agrees that it will adopt procedures to ensure the confidentiality, security, integrity, and availability of all Confidential Information provided under this Contract that is known to Contractor. Those procedures include, for each prospective and current officers, agents, employees, partners, and subcontractors of Contractor designated to work under this Contract or under any amendments hereof, that they are required:

(i) if entering state facilities through physical means, to be required to undergo the same security clearances as are required of those workforce members of the Department who physically access state facilities including, upon request by Department, submitting identifying information and being fingerprinted on-site at Contractor's expense. The Department shall arrange for the scheduling of such fingerprinting activities on Department premises; or

(ii) if using or entering state facilities through electronic, telecommunications, information technology, or any other virtual means, to be required to undergo the same security clearances as are required of those workforce members of the Department who access state facilities including, upon request by the Department, submitting identifying information and being fingerprinted at Contractor's location at Contractor's expense. Contractor shall arrange for the scheduling of such fingerprinting activities at a law enforcement agency in Contractor's locale, and in accordance with the law of the jurisdiction in which such fingerprinting takes place, either

(a) submit those fingerprints to a local law enforcement or criminal justice agency for the purpose of obtaining a criminal history record report, and, at the Department's discretion, to the Federal Bureau of Investigation for a national criminal history record check, and report to the Department the substance of the criminal record of any of the fingerprinted individuals; or

(b) mail those fingerprints to the Department for the Department to submit them for the purpose of obtaining a criminal history record report(s).

5. Accessibility of Web-based Information and Applications

Contractor is solely responsible for the administration, content, intellectual property rights, and materials at Contractor's website. Contractor is solely responsible for its actions and those of its agents, employees, resellers, subcontractors, or assigns, and agrees that neither Contractor nor any of the foregoing has any authority to act or speak on behalf of the Department. As applicable, Contractor agrees to comply with New York State Enterprise IT Policy NYS-P08-005, Accessibility of Web-Based Information and Applications, as such policy may be amended or modified, the stated purpose of which is to make State Agency web-based intranet and internet information accessible for persons with disabilities. Any web-based information and applications development, or programming delivered pursuant to this Contract or procurement, must comply with New York State Enterprise IT Policy NYS-P08-005, Accessibility of Web-Based Information and Applications as determined by quality assurance testing. Quality assurance testing may be conducted by the Department and the results of such testing, if performed, must be satisfactory to the Department before web-based information and applications will be considered a qualified deliverable under the Contract or procurement.