Appendix 10A

INFORMATION SECURITY AGREEMENT   
TEMPLATE PROVISIONS

(CLIENT-FAVORABLE)

1. DEFINITIONS

a. “Agreement” means all applicable agreements between the Client and the Supplier, including: Services Agreement, Master Service Agreement, Professional Services Subcontract Agreement, and other agreements under which Supplier Performance is required.

b. “Applicable Laws” means any applicable country, federal, state, and local law, ordinances, statute, by-law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), compulsory guidance or industry code of practice, rule of court or directives, binding court decision or precedent, or delegated or subordinate legislation, pertaining to the privacy and security of Personal Data, as each may be amended from time to time. Supplier will comply with all laws, all licenses, permits and approvals required by any government or authority, and shall comply with all applicable laws, rules, policies and procedures.

c. “Business Associate Agreement” means the separate Client document that must be executed and applies when the Supplier Processes Protected Health Information.

d. “Cardholder Data” is a category of Sensitive Personal Data and includes a cardholder’s name, full account number, expiration date, and the three-digit or four-digit security number printed on the front or back of a payment card.

e. “Client Data” means all information and data provided or made available to Supplier, including Client customer information and data, any manipulation of that data and any data or information Supplier collects, generates, or otherwise obtains in connection with its Performance under the Agreement. For clarity, to the extent Client Data contains Personal Data as defined herein, the terms related to Personal Data will also apply.

f. “Electronic Protected Health Information” or “Electronic PHI” shall have the meaning given to such term as set forth in the Business Associate Agreement.

g. “Generally Accepted Practices” means those levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-current accepted industry standards generally expected of entities performing services similar to Supplier’s.

h. “Information Security Incident” means a suspected, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

i. “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

j. “Performance” means any acts by the Supplier in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service (“SaaS”), cloud platforms or hosted services. “Perform,” “Performs,” and “Performing” shall be construed accordingly.

k. “Process” means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. “Processes” and “Processing” shall be construed accordingly.

l. “Protected Data” means Client Data and all Personal Data.

m. “Protected Health Information” or “PHI” shall have the meaning given to such term as set forth in the Business Associate Agreement and is a category of Personal Data. “Protected Health Information” includes “Electronic Protected Health Information” or “ePHI”.

n. “Representatives” means Supplier, its affiliates, and their respective officers, directors, employees, agents, contractors, subcontractors and consultants.

o. “Sensitive Personal Data” or “Special Categories of Data” means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by Applicable Law and include: information on medical or health conditions, substance use disorder information, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning a natural person’s sex life or sexual orientation, precise geolocation over time, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Client may require additional privacy responsibilities when dealing with Sensitive Personal Data, which will be appended to the Agreement or a statement of work, as applicable.

p. “Supplier” means the person or legal entity, regardless of the form of organization that has entered into an agreement with Client that may require access to Protected Data. Supplier may be defined as Subcontractor, Vendor, Supplier, Licensor, or other such defined term in the Agreement.

2. LEGAL AND REGULATORY STANDARDS

a. Supplier represents and warrants that it complies with, and that throughout the term of this InfoSec Agreement and any other Agreement it will continue to comply with, all Applicable Laws. Supplier acknowledges and agrees that Supplier is solely responsible for determining Applicable Laws, and Supplier is not relying in any manner on Client in this regard. This compliance covenant is in addition to Supplier’s obligations set forth in Appendix A to this InfoSec Agreement (Supplier Security Obligations).

b. If Supplier receives, processes, transmits or stores any Cardholder Data for or on behalf of Client, Supplier represents and warrants that information security procedures, processes, and systems will at all times meet or exceed all applicable information security laws, standards, rules, and requirements related to the collection, storage, processing, and transmission of payment card information, including those established by applicable governmental regulatory agencies, the Payment Card Industry (the “PCI”), all applicable networks, and any written standards provided by Client’s information security group to Supplier from time to time (all the foregoing collectively the “PCI Compliance Standards”).

c. If Supplier Processes Protected Health Information, the terms and conditions of Client’s Business Associate Agreement will apply to the Processing of such data.

d. If neither Applicable Laws nor this InfoSec Agreement specifically address a particular data security or privacy issue, Supplier will use appropriate, Generally Accepted Practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of the potentially affected Personal Data.

e. Supplier agrees that, in the event of a breach of this InfoSec Agreement, neither Client nor any relevant Client customer will have an adequate remedy in damages. Client or an affected customer shall therefore be entitled to seek injunctive or equitable relief to immediately cease or prevent the further use or disclosure of Personal Data and ensure compliance with all Applicable Laws.

f. In the event and to the extent that the Applicable Laws impose stricter obligations on the Supplier than the express obligations under this InfoSec Agreement, Supplier shall comply with the obligations under the Applicable Laws.

3. DATA USE AND SECURITY OBLIGATIONS

a. Supplier shall not disclose Protected Data in any manner that would constitute a violation of state or federal law or the terms of this InfoSec Agreement including, without limitation, by means of outsourcing, sharing, retransfer, or access, to any person or entity, except (i) employees or agents who actually and legitimately need to access or use Protected Data in the performance of Supplier’s duties to Client, (ii) such third parties, such as but not limited to, subcontractors, but only after such third party has agreed in writing and in advance of any disclosure, to be bound by confidentiality terms at least as stringent as the terms of this InfoSec Agreement, or (iii) any other third party approved by the Client in writing and in advance of any disclosure, but only to the extent of such approval.

b. Supplier shall only use, store, or access Protected Data (i) in accordance with, and only to the extent permissible under this Agreement and the Contract, and (ii) in full compliance with any and all Applicable Laws. Any transmission, transportation, or storage of Protected Data outside the United States is prohibited except on prior written authorization by the Client.

c. Supplier will adhere to the safeguarding and response reporting requirements set forth in Appendix A to this InfoSec Agreement.

4. CERTIFICATIONS

a. Supplier must maintain the certifications listed in the Agreement, if any, and any applicable Statement of Work (“SOW”) and Supplier shall provide annual, written, updates recertifying such certifications. If there is a material change in the requirements of a required certification or the nature of the Performance Supplier is providing, such that Supplier no longer wishes to maintain such certifications, Supplier will request such changes in writing to Client and the parties will discuss alternatives and compensating controls in good faith. Such change would allow Client to terminate any underlying Agreement(s) for cause and without penalty to Client.

b. Prior to Processing Personal Data, Supplier will provide Client with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern Supplier’s Processing of Personal Data. Supplier will promptly notify Client if Supplier has failed or no longer intends to adhere to such certifications or successor frameworks.

c. If Supplier does not maintain external certifications related to privacy or data security that are satisfactory to Client,

i. Supplier shall provide Client with documentation requested by Client sufficient to demonstrate Supplier is in compliance with this InfoSec Agreement, Applicable Laws, and the technical and organizational security measures outlined in Appendix A.

ii. Client and/or its duly authorized representatives, or in the case of a Client customer, the customer and/or its duly authorized representatives, shall have the right to conduct its own security audit of Supplier in the event of reasonable suspicion or identification of any inadequately mitigated material security related risk related to Client, Personal Data, or systems. Such audit shall be conducted with reasonable advance notice to Supplier, and shall take place during normal business hours.

5. INDEMNIFICATION

a. Supplier will defend, indemnify, and hold harmless Client and its officers, directors, employees, agents, successors, and permitted assigns from and against all third-party claims, suits, or other actions and all losses, liabilities, costs, expenses, and damages (including but not limited to reasonable attorneys’ fees, and all costs and expenses associated with data breach response and notification obligations) arising from or related to (i) any breach of Applicable Laws, including without limitation privacy and data security laws and regulations, by Supplier, its employees or agents, or (ii) any breach of this InfoSec Agreement or an Agreement by Supplier, its employees or agents.

APPENDIX A

SUPPLIER SECURITY OBLIGATIONS

Safeguarding Protected Data

Supplier agrees that use, storage, and access to Protected Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Supplier shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of Protected Data. Supplier shall also implement and maintain any safeguards required to be implemented by Applicable Laws.

Such safeguards shall include as appropriate, and without limitation, the following:

System Security. A system that is owned or operated by Supplier and contains Protected Data (“System”) shall be secured as follows:

Supplier shall implement controls reasonably necessary to prevent a breach.

The System shall use secure protocols and encryption to safeguard Protected Data in transit.

Supplier understands the System may be placed on a public network and shall implement safeguards reasonably necessary to protect its System from compromises and attacks. Supplier will protect the System with firewalls.

Supplier shall additionally:

Limit administrative access to the System,

Limit remote access to the System,

Limit account access and privileges to the least necessary for the proper functioning of the System,

Remove or disable applications and services that are not necessary for the proper functioning of the System,

Use named user accounts and not generic or shared accounts,

Use Federated Single Sign On, Kerberos, or other industry compliant services for authentication and authorization, and

Enable an appropriate level of auditing and logging for the operating system and applications.

The System shall allow the changing of System and user passwords.

Product Maintenance and Support

Supplier shall have a process for the timely review, testing, and installation of patches essential for safeguarding the confidentiality, integrity, or availability of the System or Protected Data.

Change management procedures shall be followed.

Supplier shall ensure that the product is supported, provided that Client maintains the requisite subscriptions. Supplier shall provide Client with notice 12 months before the product becomes unsupported.

If necessary, and provided that Client maintains the requisite subscriptions, Supplier shall provide remote support via a secure connection method that includes an audit log of events. Remote access shall be limited to an as-needed or as-requested basis.

Data Protections

Supplier shall implement controls reasonably necessary to prevent unauthorized use, disclosure, loss, acquisition of, or access to Protected Data. This includes, but is not limited to personnel security measures, such as background checks.

All transmissions of Protected Data by Supplier shall be performed using a secure transfer method

Supplier Access to Client Systems

Client login credentials may be given to Supplier personnel requiring access to secured computer equipment located on-site at the Client for the purposes of scheduled troubleshooting, maintenance, or updates to software provided or supplied by Supplier and installed on Client-owned computer equipment. In this case, the Client will provide the Supplier with credentials for logging in locally or through our secured Virtual Private Network (VPN), if required. Credentials will be created upon entry of a help desk ticket by the Client department for which the Supplier will be working. The Supplier credentials will be enabled for the time specified in the help desk ticket and will be disabled once that time has expired. The Client Department is responsible for notifying the Help Desk should Supplier access be no longer needed prior to the expiration date specified in the Work Ticket. Passwords will follow normal Client password policy, including 90-day password expirations, unless exceptions are granted by Information Technology for the specific case of Client credentials which are embedded into a system for automating processing or testing.

As a condition of the Supplier’s access to Client computing equipment the Supplier represents that it will not attempt to access any system(s) other than the one(s) designated in the help desk ticket nor will the Supplier use any computer equipment for any purpose that is unlawful.

All work performed by the Supplier while connected to Client computing equipment is subject to monitoring by Client staff and verification by the Client Department or Division requesting the access.

Oversight

The Client reserves the right to request security information reasonably necessary to ascertain Client’s own compliance with state and federal privacy and data security laws. Upon the Client’s request, Supplier shall provide a copy of its most recent information security audit report, and that of any data center in which Protected Data is stored.

Information Security Incident Reporting and Response

If Supplier becomes aware that Protected Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of the InfoSec Agreement or an Agreement, Supplier shall use reasonable efforts to alert the Client of any Information Security Incident within two business days, and shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the Information Security Incident. Supplier shall give highest priority to immediately correcting any Information Security Incident and shall devote such resources as may be required to accomplish that goal. Supplier shall provide the Client information necessary to enable the Client to fully understand the nature and scope of the Information Security Incident. If required by Applicable Laws, Supplier shall provide notice and credit monitoring to parties affected by any Information Security Incident. Upon request, Supplier shall provide Client information about what Supplier has done or plans to do to mitigate any deleterious effect of the unauthorized use or disclosure of, or access to, Protected Data. In the event that an Information Security Incident requires Supplier’s assistance in reinstalling software or reconstructing databases or servers, such assistance shall be provided at Supplier’s sole cost and expense. The Client may discontinue any services or products provided by Supplier until the Client, in its sole discretion, determines that the cause of the Information Security Incident has been sufficiently mitigated.