Effective October 28, 2024. This Data Processing Agreement supersedes and replaces all prior versions.

Data Processing Agreement

This Data Processing Agreement (the "Agreement") between Provider (sometimes referred to as "Provider," "we," "us," or "our"), and the Client found on the applicable Order (sometimes referred to as "you," or "your,") and, together with the Order, Master Services Agreement, Schedule of Services, and other relevant Service Attachments, forms the Agreement between the parties the terms to which the parties agree to be bound.

The parties agree as follows:

1. Health Insurance Portability and Accountability Act ("HIPAA") Data Processing. This Agreement documents the safeguards imposed upon the parties to protect health information that is subject to the Health Insurance Portability and Accountability Act ("HIPAA"). If Provider is engaged as a "Business Associate" under HIPAA, then this Agreement shall apply to Provider's activities as a Business Associate. If HIPAA applies to Provider's activities as a Business Associate, in Order to demonstrate the parties' compliance with HIPAA, this Agreement applies to each agreement between Provider or any of Provider's Affiliates and Client or any of Client's Affiliates under which Provider engages protected health information as part of its performance.

a. DEFINITIONS

The following terms used in this Agreement have the same meanings as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

- Business Associate. "Business Associate" generally has the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this Agreement, means Provider.
- Covered Entity. "Covered Entity" generally has the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this Agreement, means Client.
- HIPAA Rules. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

b. OBLIGATIONS OF BUSINESS ASSOCIATE

Business Associate agrees to:

i. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
ii. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

iii. Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;
iv. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;
v. Make available protected health information in a designated record set to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.524;
vi. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;
vii. To the extent required by regulators, maintain and make available the information required to provide an accounting of disclosures to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.528;
viii. To the extent the Business Associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and
ix. To the extent required by regulators, make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

c. PERMITTED USES AND DISCLOSURES

i. Business Associate may only use or disclose protected health information as necessary to perform the services set forth in the Master Services Agreement. The Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the Business Associate will de-identify the information and the permitted uses and disclosures by the Business Associate of the de-identified information.
ii. Business Associate may use or disclose protected health information as required by law.
iii. Business Associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures.
iv. Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity.
v. Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
vi. Business Associate may provide data aggregation services relating to the health care operations of the covered entity.

d. PRIVACY PRACTICES AND RESTRICTIONS

i. Covered entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.
ii. Covered entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the

extent that such changes may affect Business Associate's use or disclosure of protected health information.

iii. Covered entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

e. PERMISSIBLE REQUESTS

Covered entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity.

2. Gramm-Leach-Bliley Act ("GLBA") Data Processing. This section documents the safeguard standards imposed to protect Client financial information subject to the Gramm-Leach Bliley Act ("GLBA"). To the extent Provider's services constitute processing of financial information governed by GLBA, these provisions shall apply.

a. DEFINITIONS

All capitalized terms in this Addendum which are not otherwise defined in this Addendum or in the MSA have the meaning set forth in Title V of the Gramm-Leach-Bliley Act (P. L. 106-102; 15 USC §6801 et seq.) and the regulations issued pursuant thereto by the Financial Institution's Functional Regulator.

b. RECEIPT OF INFORMATION

To perform its duties under the Agreement, Provider is authorized and permitted to receive, hold and, to the extent necessary, review Nonpublic Personal Information of Client in order to provide services for Client at Client's direction as provided under the MSA. Provider may further use and disclose Nonpublic Personal Information for the proper management and administration of the business of Provider.

c. OBLIGATIONS OF SERVICE PROVIDER

Provider will take reasonable steps to:

- Implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of Nonpublic Personal Information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Client Information (16 C.F.R. § 314) and the Red Flag Rules issued by the Federal Trade Commission;
- Ensure the security and confidentiality of Nonpublic Personal Information received from Client;
- Protect against any anticipated threats or hazards to the security or integrity of Nonpublic Personal Information;
- Protect against unauthorized access to or use of such information that could result in harm or inconvenience to Client;
- Ensure the proper disposal of Nonpublic Personal Information, as set forth in the MSA or in Service Attachments signed under the MSA, and
- Notify Client of any loss or breach of the security or Confidentiality of Client's Nonpublic Personal Information.

d. PERMITTED USES AND DISCLOSURES

Provider may disclose the information received by it under the Agreement only if the disclosure is required by law.

e. PERMISSIBLE REQUESTS

Client shall not request Provider to use or disclose Nonpublic Personal Information in any manner

that would not be permissible Title V of the Gramm-Leach-Bliley Act (P. L. 106-102; 15 USC §6801 et seq.) and the regulations issued pursuant thereto if done by Client.

3. Department of Defense Standards for Controlled Unclassified Information ("CUI"). This section documents the safeguards imposed to protect CUI subject to the DoD and CMMC's standards. To the extent Provider's services involve CUI subject to DoD or CMMC standards or regulations, these provisions shall apply.

a. System Environment. Provider will prepare a detailed description of system boundaries, system interconnectedness, and key devices.

b. Requirements. Provider will thoroughly describe how the CMMC requirements have been implemented for each of the following:

i. Access Control
ii. Awareness and Training
iii. Audit and Accountability
iv. Configuration Management
v. Identification and Authentication
vi. Incident Response
vii. Maintenance
viii. Media Protection
ix. Personnel Security
x. Physical Protection
xi. Risk Assessment
xii. Security Assessment
xiii. System and Communication Protection
xiv. System and Information Integrity

c. Definitions. As used in this section —

Compromise means disclosure of information to unauthorized persons, for a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered defense information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

d. Restrictions. Provider agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) Provider shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) Provider shall protect the information against unauthorized release or disclosure.

(3) Provider shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject Provider to—

- Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and
- Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third-party beneficiary of this clause.

e. Subcontracts. The Contractor shall include this clause, including this paragraph(c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial products and commercial services, without alteration, except to identify the parties.

4. California Consumer and Privacy Act. This section documents the safeguard standards imposed to protect Client information subject to the California Consumer and Privacy Act ("CCPA"). To the extent Provider's services constitute processing of personal information governed by CCPA, these provisions shall apply.

a. DEFINITIONS

i. "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et. seq., and its implementing regulations.

ii. "Client Personal Information" means any Client Data maintained by Client and processed by Provider solely on Client's behalf, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, to the extent that such information is protected as "personal information" (or an

analogous variation of such term) under applicable U.S. Data Protection Laws.

iii. "U.S. Data Protection Laws" means all laws and regulations of the United States of America, including the CCPA, applicable to the processing of personal information (or an analogous variation of such term).

iv. "Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

b. Roles. The parties acknowledge and agree that with regard to the processing of Client Personal Information performed solely on behalf of Client, Provider is a Service Provider and receives Client Personal Information pursuant to the business purpose of providing the Services to Client in accordance with the Agreement.

c. No Sale of Client Personal Information to Provider. Client and Provider hereby acknowledge and agree that in no event shall the transfer of Client Personal Information from Client to Provider pursuant to the Agreement constitute a sale of information to Provider, and that nothing in the Agreement shall be construed as providing for the sale of Client Personal Information to Provider.

d. Limitations on Use and Disclosure. Provider is prohibited from using or disclosing Client Personal Information for any purpose other than the specific purpose of performing the Services specified in the Agreement, the permitted business purposes set under applicable law, and as required under applicable law. Provider hereby certifies that it understands the foregoing restriction and will comply with it in accordance with the requirements of applicable U.S. Data Protection Laws.

e. Data Subject Access Requests. Provider will reasonably assist Client with any data subject access, erasure or opt-out requests and objections. If Provider receives any request from data subjects, authorities, or others relating to its data processing, Provider will without undue delay inform Client and reasonably assist Client with developing a response (but Provider will not itself respond other than to confirm receipt of the request, to inform the data subject, authority or other third party that their request has been forwarded to Client, and/or to refer them to Client, except per reasonable instructions from Client). Provider will also reasonably assist Client with the resolution of any request or inquiries that Client receives from data protection authorities relating to Provider, unless Provider elects to object such requests directly with such authorities.

f. Data Retention. Provider will retain only the minimum amount of data that is essential to fulfill its obligations under the Master Services Agreement, Service Attachments, and this DPA. Provider will not keep data longer than is necessary without first providing notice to the Client with a justification of the extended retention.

5. Colorado Privacy Act. This section documents the safeguard standards imposed to protect Client information subject to the Colorado Privacy Act (6-1-1301) ("CPA"). To the extent Provider's services constitute processing of personal information governed by CPA, these provisions shall apply.

Provider shall adhere to the instructions of the controller and assist the controller to meet its obligations under the CPA.

Taking into account the nature of processing and the information available to Provider, Provider shall assist the controller by:

a. taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6-1-1306;

b. helping to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 6-1-716; and

c. providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 6-1-1309.

Notwithstanding the instructions of the controller, Provider shall:

a. ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and
b. engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

Taking into account the context of processing, Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between Provider and the controller to implement the measures.

Processing by Provider must be governed by a contract between the controller and Provider that is binding on both parties and that sets out:

a. the processing instructions to which the processor is bound, including the nature and purpose of the processing;
b. the type of personal data subject to the processing, and the duration of the processing; and
c. the following requirements:
    (i) at the choice of the controller, Provider shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

    (ii) (a) Provider shall make available to the controller all information necessary to demonstrate compliance with the obligations; and

    (b) Provider shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, Provider may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at Provider's expense, an audit of the Provider's policies and technical and organizational measures in support of its obligations under the CPA using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. Provider shall furnish a report of the audit to the controller upon request.

6. **Connecticut Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Connecticut SB 12-2 ("Conn Act"). To the extent Provider's services constitute processing of personal information governed by Conn Act, these provisions shall apply.

Provider shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under the Conn Act. Such assistance shall include:

a. taking into account the nature of processing and the information available to Provider, providing appropriate technical and organizational measures to fulfill the controller's obligation to respond to consumer rights requests;

b. taking into account the nature of processing and the information available to Provider, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of Provider's systems, in order to meet the controller's obligations; and

c. providing necessary information to enable the controller to conduct and document data protection assessments.

Provider shall have a written contract with the controller that will govern the Provider's data-processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that Provider:

a. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

b. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

c. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate Provider's compliance with the obligations

d. after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of Provider with respect to the personal data; and

e. allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of Provider's policies and technical and organizational measures in support of the obligations of the Conn Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments.

Provider shall provide a report of such assessment to the controller upon request.

For purposes of the Conn Act, the following definitions apply:

a. "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

b. "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

c. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

d. "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

e. "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller

7. New York SHIELD

Provider maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Provider's business; (b) the amount of resources available to Provider; (c) the type of information that Provider will store; and (d) the need for security and confidentiality of such information. The Data Processing Agreement may be updated by Provider from time-to-time.

Provider's security program is designed to:

- Protect the confidentiality, integrity, and availability of Customer Data or Professional Services Data in Provider's possession or control or to which Provider has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data or Professional Services Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data or Professional Services Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data or Professional Services Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Provider may be regulated.

Without limiting the generality of the foregoing, Provider's security program includes:

1. **Security Awareness and Training**. A mandatory security awareness and training program for all members of Provider's workforce (including management), which includes:
   a) Training on how to implement and comply with its Information Security Program;
   b) Promoting a culture of security awareness through periodic communications from senior management with employees.

2. **Access Controls**. Policies, procedures, and logical controls:
   a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
   b) To prevent those workforce members and others who should not have access from obtaining access; and
   c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the production data center or the facility housing Provider's SFTP Server, if applicable, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include:
   a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
   b) Camera surveillance systems at critical internal and external entry points to the data center;
   c) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
   d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any Security Breach. Such procedures include:
   a) Roles and responsibilities: formation of an internal incident response team with a response leader;
   b) Investigation: assessing the risk the incident poses and determining who may be affected;
   c) Communication: internal reporting as well as a notification process in the event of unauthorized disclosure

of Customer Data or Professional Services Data;
d) Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and
e) Audit: conducting and documenting root cause analysis and remediation plan.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

   a) Data Backups: A policy for performing periodic backups of production file systems and databases or Professional Services Data on Provider's SFTP Server, as applicable, according to a defined schedule;
   b) Disaster Recovery: A formal disaster recovery plan for the production data center, including:
      i) Requirements for the disaster plan to be tested on a regular basis, currently twice a year; and
      ii) A documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to customers.
   c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

6. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Data or Professional Services Data and protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Customer Data or Professional Services Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Customer Data or Professional Services Data stored on desktops, laptops or other removable storage devices.

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Customer Data or Professional Services Data, taking into account available technology so that Customer Data or Professional Services Data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including:
    a) Designating a security official with overall responsibility;
    b) Defining security roles and responsibilities for individuals with security responsibilities; and
    c) Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:
    a) Reviewing changes affecting systems handling authentication, authorization, and auditing;
    b) Reviewing privileged access to Provider production systems; and
    c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Provider makes to production systems, applications, and databases. Such policies and procedures include:
    a) A process for documenting, testing and approving the patching and maintenance of the Service;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and
c) A process for Provider to utilize a third party to conduct web application-level security assessments. These assessments generally include testing, where applicable, for:
   i) Cross-site request forgery
   ii) Services scanning
   iii) Improper input handling (e.g., cross-site scripting, SQL injection, XML injection, cross-site flashing)
   iv) XML and SOAP attacks
   v) Weak session management
   vi) Data validation flaws and data model constraint inconsistencies
   vii) Insufficient authentication
   viii) Insufficient authorization

14. **Program Adjustments**. Provider monitors, evaluates, and adjusts, as appropriate, the security program in light of:
   a) Any relevant changes in technology and any internal or external threats to Provider or the Customer Data or Professional Services Data;
   b) Security and data privacy regulations applicable to Provider; and
   c) Provider's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

15. **Devices**. All laptop and desktop computing devices utilized by Provider and any subcontractors when accessing Customer Data or Professional Services Data:
   a) will be equipped with hard disk drive encryption;
   b) will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and
   c) shall maintain virus and malware detection and prevention software so as to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by supplier of such software.

Definitions

"Professional Services" means consulting or professional services provided to Customer under an agreement between the parties for the provision of consulting or professional services.

"**Professional Services Data**" means electronic data or information that is provided to Provider under a Professional Services engagement with Provider for the purpose of being input into the Provider Service, or Customer Data accessed within or extracted from the Customer's tenant to perform the Professional Services.

"**SFTP Server**" means a Secure File Transfer Protocol server or its successor provided and controlled by Provider to transfer the Professional Services Data between Customer and Provider for implementation purposes.

8. **Virginia Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Code of Virginia Section 59.1-579 ("VPA"). To the extent Provider's services constitute processing of personal information governed by VPA, these provisions shall apply:

.

   a. This DPA sets forth instructions for the following:
      i. Provider may provide hosting services and will only process data that is deposited by Client into Provider's systems;
      ii. Provider will not use non-anonymized protected data for any of its own business purposes;
      iii. Any processing will be for a reasonable amount of time given the Services to be performed; and
      iv. Both Provider and Client have the right to adjust whether Client may deposit protected data into Provider's systems.

b. With respect to the protected data, Provider shall:

- **i.** Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- **ii.** At the Client's direction, delete or return all protected data to the Client as requested at the end of the provision of services, unless retention of the protected data is required by law;
- **iii.** Upon the reasonable request of the Client, make available to the Client all information in its possession necessary to demonstrate the Provider's compliance with the obligations in this chapter;
- **iv.** Allow, and cooperate with, reasonable assessments by the Client the Client's designated assessor; alternatively, Provider may arrange for a qualified and independent assessor to conduct an assessment of the Provider's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Provider shall provide a report of such assessment to the Client upon request; and
- **v.** Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the Provider with respect to the protected data.