Effective March 14, 2023. This Data Processing Agreement supersedes and replaces all prior versions.

Data Processing Agreement

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

The parties agree as follows:

1. 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.

2. 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 Security Exhibit 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.

STATEMENT OF WORK

The subject matter and duration of the Processing, the nature and purpose of the Processing, and the type of Personal Data and categories of data subjects will be described in a statement of work, purchase order or written agreement signed by the parties' authorized representatives, which forms an integral part of the Agreement.

INSURANCE

In addition to any other insurance required under the Agreement, Client will maintain insurance coverage for privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to data breaches, and legal claims for security breach, privacy violations, and notification costs) of at least $2,000,000 US per occurrence.

TERM AND TERMINATION

(a) Term. The Term of this Agreement shall be effective as of the date signed by both parties below, and shall terminate upon the termination of the Agreement or upon the date Client terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Provider authorizes termination of this Agreement by Client, if Client determines Provider has violated a material term of the Agreement and Provider has not cured the breach or ended the violation within ten (10) business days.

(c) Effect of Termination. Upon termination of this Agreement for any reason, Provider, with respect to Personal Data received from Client, or created, maintained, or received by Provider on behalf of Client, shall:

(i) Retain only that Personal Data which is necessary for Provider to continue its proper management and administration or to carry out its legal responsibilities;

(ii) Return to Client the remaining Personal Data that the Provider still maintains in any form;

(iii) Continue to use appropriate safeguards with respect to Personal Data to prevent use or disclosure of the Personal Data, other than as provided for in this Section, for as long as Provider retains the Personal Data;

(iv) Not use or disclose the Personal Data retained by Provider other than for the purposes for which such Personal Data was retained and subject to the same conditions set forth in this Agreement; and

(v) Return to Client the Personal Data retained by Provider when it is no longer needed by Provider for its proper management and administration or to carry out its legal responsibilities.

In addition, Client's termination of this Agreement for cause constitutes good cause for Client to terminate any Service Attachments signed under the Agreement in connection with which Provider received any Personal Data from Client.

(d) Survival. The obligations of Provider under this Section shall survive the termination of this Agreement.