Data Security Policy

1. **Definitions** Capitalized terms used herein shall have the meanings set forth in this Section 1.

(a) "***Authorized Persons***" means Company's employees, contractors, agents, and auditors who have a need to know or otherwise access Personal Information to enable Company to perform its obligations under this Agreement, and who are bound in writing by confidentiality and other obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Agreement.

(b) "***Personal Information***" means information that Customer provides or for which Customer provides access to Company, or information which Company creates or obtains on behalf of Customer, in accordance with this Agreement that: (i) directly or indirectly identifies an individual; or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, user identification and account access credentials or passwords, financial account numbers, credit report information, student information, biometric, genetic, health, or health insurance data, answers to security questions, and other personal identifiers), in case of both subclauses (i) and (ii), including Sensitive Personal Information as defined in Section 1(c). Customer's business contact information is not by itself Personal Information.

(c) "***Sensitive Personal Information***" means an individual's (i) government-issued identification number, including Social Security number, driver's license number, or state-issued identification number; (ii) financial account number, credit report information, or credit, debit, or other payment cardholder information, with or without any required security or access code, personal identification number, or password that permits access to the individual's financial account; or (iii) biometric, genetic, health, or health insurance data.

(d) "***Data Breach***" means any act or omission that materially compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place by Company (or any Authorized Persons), or by Customer should Company have access to Customer's systems, that relate to the protection of the security, confidentiality, or integrity of Personal Information, or (ii) receipt of a complaint in relation to the privacy and data security practices of Company (or any Authorized Persons)or a breach or alleged breach of this Agreement relating to such privacy and data security practices.

2. **Company and Customer Obligations**

(a) Company will:

(i) comply with the terms of this Policy.

(ii) be responsible for any unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Personal Information under its control or in its possession by all Authorized Persons.

(iii) not disclose Personal Information to any person other than its Authorized Persons without Customer's prior written consent unless required by applicable law, in which case, Company will use reasonable efforts and to the extent permitted by applicable law notify Customer before such disclosure or as soon thereafter as reasonably possible.

(iv) use and disclose Personal Information only for the purposes for which Customer provides the Personal Information, or access to it, pursuant to the terms and conditions of this Policy, and not use or otherwise disclose or make available Personal Information for Company's own purposes without Customer's prior written consent.

(b) Customer will:

(i) comply with the terms and conditions set forth in this Policy.

(ii) be responsible for any unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Personal Information under its control or in its possession.

(iii) comply with any applicable laws and regulations and use only secure methods, according to accepted industry standards, when transferring or otherwise making available Personal Information to Company or transmitting Personal Information using the System.

(iv) provide written notice to Company if any information Customer provides to Company under this Policy contains Personal Information. Company will not be responsible for determining on its own that any information Customer provides under this Policy qualifies as Personal Information.

3. **Information Security**

(a) Company will comply with applicable laws and regulations in its creation, collection, receipt, access, use, storage, disposal, and disclosure of Personal Information.

(b) Company will employ reasonable security measures to protect Personal Information in accordance with Company's information security policy as amended from time to time ("***Information Security Policy***").

(c) If, in the course of its performance under this Policy, Company has access to or will collect, access, use, store, process, dispose of, or disclose credit, debit, or other payment cardholder information on Customer's behalf, Company will comply with the Payment Card Industry Data Security Standard ("***PCI DSS***") requirements, as applicable.

4. **Data Breach Procedures**

(a) Company will notify Customer of a Data Breach as soon as reasonably practicable after Company becomes aware of it.

(b) Immediately following Company's notification to Customer of a Data Breach, the parties will coordinate with each other, as necessary, to investigate the Data Breach in accordance with commercially reasonable standards.

(c) Company agrees that it will not inform any third party of any Data Breach without Customer's prior consent, other than to inform a complainant that the matter has been forwarded to Customer's legal counsel.

5. **Return or Disposal of Personal Information**

At any time during the term of this Policy at Customer's written request or on the termination of any services provided by Company to Customer, Company will promptly return to Customer or securely dispose of all Personal Information in its possession and notify Customer that such Personal Information has been returned to Customer or disposed of securely. If Company is not reasonably able to return or securely dispose of Personal Information, including, but not limited to, Personal Information stored on backup media, Company will continue to protect such Personal Information in accordance with the terms of this Policy until such time that it can reasonably return or securely dispose of such Personal Information.