These are samples of language that can be used in a vendor agreement for the use, storage or processing of personal information by the vendor.

Definitions

"Authorized Persons" means the Service Provider's employees, contractors, agents, or auditors, who Service Provider determines has a need to access Personal Information or confidential information to enable Service Provider to perform its obligations to Customer under this Agreement, and who will agree to be bound in writing by confidentiality obligations sufficient to protect Personal Information or confidential information.

"Personal Information" means and includes any information provided to Service Provider by Customer or at Customer's direction, that either (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, Social Security Numbers (SSNs), employee identification numbers, government-issued identification numbers, passwordsor PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers).

"Data Breach" means any act or omission that compromises either the security, confidentiality or integrity of Personal Information.

"Data Incident" means any act or omission that may materially compromise the physical, technical or administrative safeguard put in place by the Service Provider but that does not result in a Data Breach.

Safeguard of Personal Information

Service Provider agrees and covenants that it shall (i) keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure; (ii) use Personal Information solely and exclusively for the purpose for which Personal Information solely and exclusively for the purposes for which Customer shares or provides it to Service Provider, and shall not use, transfer, sell, rent, distribute or otherwise disclose Personal Information for the Service Provider's benefit or for any other purpose without Customer's prior written consent; (iii) shall not directly or indirectly disclose Personal Information to anyone other than its Authorized Persons without express written prior consent from Customer, unless and to the extent required by law.

Information and Data Security

Service Provider warrants and represents that its access, collection, storage and disposal of Personal Information does and shall comply with applicable federal and state statutes and regulations.

Without limiting Service Provider's obligations pursuant to this Agreement, Service Provider shall implement administrative, physical and technical safeguards for protection of Personal Information that are no less rigorous than acceptable industry practices, including but not limited to [insert applicable standard for industry, if necessary], and shall ensure that all such safeguards comply with applicable data protection and privacy laws, statutes and regulations.

During the term of this Agreement, and until Customer's information is Service Provider shall at all times cause Authorized Persons to abide strictly by Service Provider's obligations pursuant to this Agreement, and its internal policies and procedures, copies of which are attached to this Agreement and incorporated by reference into this Agreement.

Data Breach or Data Incident Procedures

In the event of a Data Breach or Data Incident, Service Provider shall (i) notify Customer of a Data Breach as soon as practicable, but no later than [ ] hours after Service Provider becomes aware of the Data Breach and (ii) notify Customer of a Data Incident promptly after Service Provider determines that the Data Incident did not rise to the level of a Data Breach. Immediately following the Service Provider's notification to customer of a Data Breach, Service Provider and Customer shall coordinate to investigate the Data Breach. Service Provider shall bear all costs and expenses of the investigation and reporting of Data Breach caused by Service Provider, and shall cooperate with Customer's personnel, including any insurance carriers to which Customer reports the incident, fully, including, without limitation, by providing access to Customer and/or its personnel or carriers, to relevant records, logs, files, data reporting or other materials requested.

Service Provider expressly agrees that it shall not inform any third party, including law enforcement, consumer reporting agencies, or affected employees or consumers, of any Data Breach without first notifying Customer, other than to inform a complainant that the matter has been forwarded to Customer's counsel. Customer shall have the sole right to determine whether notice of the Data Breach shall be reported to third parties, including law enforcement, consumer reporting agencies or as otherwise required, and Customer shall have the sole discretion over the contents of any such notice. Service Provider shall undertake any instructed notice at its sole expense.

Compliance Oversight

Upon written request from Customer, Service Provider shall confirm compliance with this Agreement and any applicable industry standards, and shall promptly provide to Customer a written information security questionnaire regarding Service Provider's information technology resources, data security protocols and applicable policies. Failure to provide such information shall be grounds for Customer to terminate this Agreement immediately.

Return of Confidential Information

At any time during the term of this Agreement, or upon Customer's written request, or upon the termination of this Agreement, Service Provider shall instruct all Authorized Persons to promptly return to Customer all copies, whether in written, electronic or other form of media, of Personal Information or confidential information, in its possession, custody or control, and certify in writing to Customer that such Personal Information or confidential information has been returned to Customer or disposed of securely.

Material Breach

Service Provider acknowledges that any breach of the provisions of this section regarding Service Provider's data security measures is a material breach of this Agreement. As such, Customer may terminate this Agreement effective immediately upon written notice to the Service Provider without any further liability or obligation to Customer.

Equitable Relief

Service Provider acknowledges that any breach of the provisions of this section regarding Service Provider's data security may cause Customer irreparable harm, for which monetary damages will not be adequate compensation. Service Provider therefore agrees that Customer may seek equitable relief, including but not limited to injunctive relief or specific performance, to enforce the terms of this Agreement. Such equitable relief is not exclusive, but rather, is in addition to all other remedies available at law or in equity, subject to the terms of this Agreement.

Indemnification

Service Provider shall defend, indemnify and hold harmless Customer, and [its/their] subsidiaries, affiliates, and [its/their] respective officers, directors, employees, agents, successors and permitted assigns] (each, a **"Customer Indemnitee"**) from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third- party claim against any Customer Indemnitee arising out of or resulting from Service Provider's failure to comply with any of its obligations under this Section.