ECKERT SEAMANS
ATTORNEYS AT LAW

Sample Contract Clauses

By Stephen M. Foxman, Esq.

Disclaimer: **The following clauses are examples of actual data protection clauses used in technology agreements, adapted to remove any identifying information regarding the providers or customers. Use and final language of the following clauses must be modified to be appropriate for any specific software or service being provided by a licensor, vendor or service provider. Such clauses should not be used without advice from a lawyer familiar with technology agreements and data protection issues. Close attention must also be paid to any disclaimer or limitation of liability clauses, which may undermine the effectiveness of remedies related to any breach by any licensor, vendor or service provider of its contractual obligations.**

Short and Concise Data Protection Clause:

Data Protection. Licensor acknowledges that it may have access to certain of Licensee's computer and communications systems and networks for the purposes set forth in this Agreement. If any data is made available or accessible to Licensor, its employees, agents or contractors, pertaining to Licensee's business or financial affairs, or to Licensee's projects, transactions, clients or customers, Licensor will not store, copy, analyze, monitor or otherwise use that data except for the purposes set forth in the License Agreement for the benefit of Licensee. Licensor will comply fully with all applicable laws, regulations, and government orders relating to personally identifiable information ("PII") and data privacy with respect to any such data that Licensor receives or has access to under the License Agreement or in connection with the performance of any services for Licensee. Licensor will otherwise protect PII and will not use, disclose, or transfer across borders such PII except as necessary to perform under the License Agreement or as authorized by the data subject or in accordance with applicable law. To the extent that Licensor receives PII related to the performance of the License Agreement, Licensor will protect the privacy and legal rights of Licensee's personnel, clients, customers and contractors.

Comprehensive Data Protection Clauses (Including Exhibit Language):

Customer Data and Intellectual Property. All right, title, and interest in Customer Data (as defined below) will remain the property of Customer. Licensor has no intellectual property rights or other claim to Customer Data that is hosted, stored, or transferred to and from the Products or the cloud services platform provided by Licensor, or to Customer's Confidential Information. Licensor will cooperate with Customer to protect Customer's intellectual property rights and Customer Data. Licensor will promptly notify Customer if Licensor becomes aware of any potential infringement of those rights in accordance with the provisions of this Agreement.

Security and Data Protection.

1. Customer Data and Security. All Customer Data that will be hosted by Licensor under this Agreement will be hosted at data centers maintained and operated by [insert name] located in [insert location address or addresses] (the " Data Centers"). For purposes of this Agreement and the Exhibits attached hereto "Customer

Data" shall include any Customer Confidential Information, and any personally identifiable information relating to any customers, end users or employees of Customer, its suppliers or contractors (" Personal Data"), to which Licensor has or may have access in connection with the operation or administration of Licensor's platform, or in connection with the performance of Professional Services by Licensor for Customer under this Agreement or any applicable Statement(s) of Work. All Customer Data stored or at rest in the Data Centers, or in transport, will be encrypted in transport and will not be transferred to any other hosting entity or location without the prior written consent of Customer.

Licensor will provide the following available services and functions as part of the Software without additional cost: (i) the use of encryption technology to protect Customer Data from unauthorized access; and (ii) routine back-up and archiving of Customer Data. Licensor will comply with the requirements of Exhibit __ (Data Security) and implement the Data Safeguards set forth in this Section, and Licensor will further implement reasonable security standards that it determines are necessary, but in no event less than industry standards, to protect (i) the physical security of the Data Centers used to maintain Customer Data; and (ii) Licensor's network, all operating systems and software applications, and all data storage systems and media provided by Licensor or its licensors or contractors, or operated or provided by Customer that connect or interface with Licensor's Products, Software or platform, from being subject to any Disabling Devices (as defined in Exhibit __ (Data Security) attached to this Agreement).

2. Data Safeguards. Licensor has represented to Customer that Licensor will not be permitted to access Customer Data stored or contained in the Products or Licensor's platform, and Licensor will have no ability to manipulate, modify or control such Customer Data. If any support services or Professional Services provided by Licensor may involve Licensor or its personnel having or requiring access to Customer servers, Customer applications, and/or Customer Data, Licensor shall comply with the provisions of this Section and Exhibit __ (Data Security) attached hereto, and, at Customer's request, Licensor shall enter into an appropriate separate agreement with Customer to govern such access and protect any Customer Data that may be subject to such access. To the extent Customer grants Licensor access to Customer Data, or Licensor has access to or stores or holds any Customer Data, Licensor agrees to:

(i) access and use the Customer Data solely for the purpose of providing Customer with access to the Products, Software and Licensor's platform, and to provide Professional Services to Customer in accordance with the terms and conditions of this Agreement and any applicable Statement(s) of Work;

(ii) maintain physical, technical, and administrative safeguards (including but not limited to those set forth in this Section, Exhibit __ (Data Security) attached to this Agreement, and in any event no less than industry standards in the cloud computing/online services industry) to protect the Customer Data against unauthorized access, use, or disclosure while it is accessible to or held by Licensor (" Data Safeguards"); and

(iii) not disclose the Customer Data to any third party, except: (x) to its employees, consultants or contractors who need to have access to such information and solely for purposes of providing Professional Services to Customer, provided that such recipients are bound by confidentiality provisions no less restrictive than those set out in this Agreement; and (y) to the extent required by a judicial order or other legal obligation, provided that, to the fullest extent permitted by law, Licensor will promptly notify Customer of such a required disclosure to allow intervention by Customer (and will cooperate with Customer) to contest or minimize the scope of the disclosure.

ECKERT SEAMANS
ATTORNEYS AT LAW

3. **SOC 1/SSAE 16 Certification**. Licensor will, on at least an annual basis, hire a third party auditing firm to perform a Statement on Standards for Attestation Engagements (SSAE) No. 16 audit, or equivalent audit, on internal and external Licensor procedures and systems that access or contain Customer Data. Licensor shall adhere to SOC 1/SSAE 16 audit compliance criteria and data security procedures (or any successor report of a similar nature that is generally accepted in the industry and utilized by Licensor), applicable to Licensor. Licensor's security procedures will materially conform to the description thereof set forth in this Agreement and in attached Exhibit __ (Data Security), and as further described in Licensor's most recently completed SOC 1/SSAE 16 audit report (or any successor report of a similar nature that is generally accepted in the industry and utilized by Licensor). Upon Customer's request, Licensor will provide Customer with a copy of the audit results set forth in Licensor's SOC 1/SSAE 16 audit report.

4. Data Breach. Licensor further agrees that it will monitor and test its Data Safeguards from time to time, and further agrees to adjust its Data Safeguards from time to time in light of relevant circumstances or the results of any relevant testing or monitoring. If Licensor suspects or becomes aware of any unauthorized access to any Customer Data or Personal Data by any unauthorized person or third party, or becomes aware of any other security breach relating to Personal Data held or stored by Licensor under this Agreement or in connection with the performance of the Professional Services or other services performed under this Agreement or any Statement(s) of Work ("Data Breach"), Licensor shall immediately notify Customer in writing and shall fully cooperate with Customer at Licensor's expense to prevent or stop such Data Breach. In the event of such Data Breach, Licensor shall fully and immediately comply with applicable laws, and shall take the appropriate steps to remedy such Data Breach. Licensor will defend, indemnify and hold Customer, its Affiliates, and their respective officers, directors, employees and agents, harmless from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorney fees, arising out of or relating to any third party claim arising from breach by Licensor of its obligations contained in this Section, except to the extent resulting from the acts or omissions of Customer. All Personal Data to which Licensor has access under this Agreement, as between Licensor and Customer, will remain the property of Customer. Customer hereby consents to the use, processing and/or disclosure of Personal Data only for the purposes described herein and to the extent such use or processing is necessary for Licensor to carry out its duties and responsibilities under this Agreement, any applicable Statement(s) of Work, or as required by law. Licensor will not transfer Personal Data to third parties other than through its underlying network provider to perform its obligations under this Agreement. All Personal Data delivered to Licensor shall be stored in the United States or other jurisdictions approved by Customer in writing and shall not be transferred to any other countries or jurisdictions without the prior written consent of Customer.

Date Security Exhibit:

EXHIBIT __
Data Security

Notwithstanding anything to the contrary contained in the Master Services and License Agreement to which this Exhibit is attached ("Agreement"), and all other Exhibits thereto, and in addition to and not in lieu of other provisions in the Agreement and the Exhibits thereto, Licensor agrees as follows:

1. General Security Procedures

1.1 Without limiting Licensor's obligation of confidentiality as further described in the Agreement and herein, Licensor will be responsible for establishing and maintaining an information security program that is designed to: (i) ensure the security and confidentiality of Customer Data; (ii) protect against any anticipated threats or hazards

to the security or integrity of the Customer Data; (iii) protect against unauthorized access to or use of the Customer Data; (iv) ensure the proper disposal of Customer Data, as further defined herein; and (v) ensure that all subcontractors of Licensor, if any, comply with all of the foregoing. Licensor will designate an individual to be responsible for the information security program. Such individual will respond to Customer inquiries regarding computer security and to be responsible for notifying Customer-designated contact(s) if a breach or an incident occurs, as further described herein. The information security program will be audited annually as detailed in Licensor's SSAE 16 and/or SOC 1 audit reports, which will be made available to Customer upon request.

1.2 Licensor must conduct formal security awareness training, with a testing component, for all personnel and contractors as soon as reasonably practicable after the time of hiring or prior to being appointed to work on Customer Data and annually recertified thereafter. Documentation of Security Awareness Training must be retained by Licensor, confirming that this training and subsequent annual recertification process have been completed, and available for review by Customer.

1.3 Customer will have the right to review Licensor's information security program prior to the commencement of Customer's entry of data into the Products or delivery to Customer of any Professional Services and from time to time during the Term of this Agreement. During the Term of the Agreement, from time to time with proper notice and Licensor approval, which will not be unreasonably withheld, Customer, at its own expense, will be entitled to perform, or to have performed, an on-site audit of Licensor's information security program and facilities. In lieu of an on-site audit, upon request by Customer, Licensor will use reasonable efforts to complete, within forty-five (45 days) of receipt, an Information Security Assessment questionnaire provided by Customer regarding Licensor's information security program.

1.4 In the event of any actual or apparent theft, unauthorized use or disclosure of any Customer Data, Licensor will immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and within two (2) business days following discovery of any such event, provide Customer notice thereof, and such further information and assistance as may be reasonably requested.

1.5 Customer Data, including but not limited to sales data, hosted, stored, or held by Licensor in the Product(s) or in the platform operated by Licensor, or on any device owned or in the custody of Licensor, its employees, agents or contractors, will be encrypted. Licensor will not transmit any unencrypted Customer Data over the internet or a wireless network, and will not store any Customer Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software approved by Customer.

1.6 The parties acknowledge and agree that any disclosure of Customer Data will in no way be construed to be an assignment, transfer, or conveyance of title to or ownership rights in such Customer Data.

2. Network and Communications Security

2.1 All Licensor connectivity to Customer computing systems and all attempts at same will be only through Customer's security gateways/firewalls and only through Customer-approved security procedures.

2.2 Licensor will not access, and will not permit unauthorized persons or entities to access, Customer computing systems and/or networks without Customer's express written authorization, and any such actual or attempted access will be consistent with any such authorization.

2.3 Licensor will take appropriate measures to ensure that Licensor's systems connecting to Customer's systems and anything provided to Customer through such systems do not contain any Disabling Device. For

purposes of this Agreement, "Disabling Device" means any programs, mechanisms, programming devices, malware or other computer code (i) designed to disrupt, disable, harm, or otherwise impede in any manner the operation of any software program or code, or any computer system or network (commonly referred to as "malware", "spyware", "viruses" or "worms"); (ii) that would disable or impair the operation thereof or of any software, computer system or network in any way based on the elapsing of a period of time or the advancement to a particular date or other numeral (referred to as "time bombs", "time locks", or "drop dead" devices); (iii) is designed to or could reasonably be used to permit a party or any third party to access any computer system or network (referred to as "trojans", "traps", "access codes" or "trap door" devices); or (iv) is designed to or could reasonably be used to permit a party or any third party to track, monitor or otherwise report the operation and use of any software program or any computer system or network by the other party or any of its customers.

3. Customer Data Handling Procedures

Erasure of Information and Destruction of Electronic Storage Media. If Customer Data is required to be permanently deleted from any storage media owned or operated by Licensor, all electronic storage media containing Customer Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization. Licensor must maintain documented evidence of data erasure and destruction. This evidence must be available for review at the request of Customer.

4. Physical Security

All backup and archival media containing Customer Data must be contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by Licensor and all backup and archival media containing Customer Data must be encrypted.

5. Penetration Testing

Licensor will provide Customer with an annual, third party Penetration Test report. During the term of this Agreement, Licensor will engage, at its own expense and at least one time per year, a third party vendor reasonably acceptable to Customer to perform penetration and vulnerability testing ("**Penetration Tests**") with respect to Licensor's systems. The objective of such Penetration Tests is to identify design and/or functionality issues in infrastructure of Licensor's systems that could expose Customer Data and its computer and network equipment and systems to risks from malicious activities. Penetration Tests will probe for weaknesses in network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to Licensor's systems that could be exploited by a malicious party. Penetration Tests will identify, at a minimum, the following security vulnerabilities: invalidated or unsanitized input; broken access control; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; denial of service; insecure configuration management; proper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing. Within a reasonable period after the annual Penetration Test has been performed, Customer may request from Licensor a report of any high level and medium level security issues that were revealed during such Penetration Test and subsequent certification in writing to Customer that such high level and medium level security issues have been fully remediated. To the extent that high level and/or medium level security issues were revealed during a particular Penetration Test, Licensor will subsequently engage, at its own expense, the Testing Customer to perform an additional Penetration Test within a reasonable period thereafter to ensure continued resolution of identified security issues and will notify Customer with the results thereof.

6. Background Checks

Licensor will perform background checks on all Licensor personnel and direct hire contractors including temporary and non-employee personnel who will be performing services for Customer, including but not limited to implementation services under any Statement(s) of Work, that requires access to Customer Data pursuant to this Agreement. Licensor will not assign any employee to perform services for Customer who has not authorized a background investigation, or whose background investigation has revealed the conviction of a felony or misdemeanor within the previous seven (7) years, measured back from the time such Licensor employee commences services pursuant to the Agreement, to the extent such felony or misdemeanor relates to the suitability of the individual's employment, except to the extent prohibited by applicable law. If Licensor contracts, for any services, with a third party that needs to be allowed or requires access to Customer Data, the third party will undergo the same Licensor background checks as performed on Licensor personnel and contractors under this section.

7. SSAE-16/SOC-1

Customer shall have the right to terminate this Agreement (together with any related agreements, including licenses and/or Statement(s) of Work) and receive a full refund for all monies prepaid thereunder in the event that Licensor fails to produce an acceptable SSAE-16/ SOC-1 Type II report.

[End of Exhibit Language]

Information Security Breach Notification Clause.

[Cloud Provider] agrees to notify Customer within two (2) business days in writing of any discovery by [Cloud Provider] of any breach or suspected breach of the provisions of this Agreement or any loss or unauthorized use, disclosure, acquisition of or access to any Customer Confidential Information and/or Customer's business systems of which [Cloud Provider] becomes aware (any such breach or suspected breach being referred to herein as a "Data Breach"). Such notice shall summarize in reasonable detail the effect on Customer, if known, of the Data Breach and the corrective action taken or to be taken by [Cloud Provider]. [Cloud Provider] shall promptly take all appropriate or legally required corrective actions, and shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Data Breach. In addition to the notice requirement contained herein, [Cloud Provider] will also immediately report any such Data Breach to Customer's Legal Department at [insert telephone number or address]

Insurance Clause for Cyber-liability Insurance.

[Service Provider] agrees to purchase and maintain throughout the term of this Agreement a technology/professional liability insurance policy, including coverage for network security/data protection liability insurance (also called "cyber liability") covering liabilities for financial loss resulting or arising from acts, errors, or omissions, in rendering technology/professional services or in connection with the specific services described in this Agreement:

ECKERT SEAMANS
ATTORNEYS AT LAW

Violation or infringement of any right of privacy, including breach of security and breach of security/privacy laws, rules or regulations globally, now or hereinafter constituted or amended;

Data theft, damage, unauthorized disclosure, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information in whatever form, transmission of a computer virus or other type of malicious code; and participation in a denial of service attack on third party computer systems;

Loss or denial of service;

No cyber terrorism exclusion;

with a minimum limit of $5,000,000 each and every claim and in the aggregate. Such coverage must include technology/professional liability including breach of contract, privacy and security liability, privacy regulatory defense and payment of civil fines, payment of credit card provider penalties, and breach response costs (including without limitation, notification costs, forensics, credit protection services, call center services, identity theft protection services, and crisis management/public relations services).

Such insurance must explicitly address all of the foregoing without limitation if caused by an employee of [Service Provider] or an independent contractor working on behalf of [Service Provider] in performing services under this Agreement. Policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world. Such insurance must include affirmative contractual liability coverage for the data breach indemnity in this Agreement for all damages, defense costs, privacy regulatory civil fines and penalties, and reasonable and necessary data breach notification, forensics, credit protection services, public relations/crisis management, and other data breach mitigation services resulting from a breach of confidentiality or breach of security by or on behalf of [Service Provider].

_____

Stephen M. Foxman
ECKERT SEAMANS
215.851.8422 sfoxman@eckertseamans.com