DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into between the Client and MyWorkplace to the extent it is incorporated into an Agreement or the Terms between you and MyWorkplace. Capitalized words in this DPA shall have the same definition as in the Agreement or the Terms unless otherwise defined herein. This DPA shall control in the event of a conflict with the Terms or the Agreement.

1 **Definitions**:

a. "**Client Data**" shall mean Client's Confidential Information and Personal Information.

b. "**Confidential Information**" shall mean any non-public information of one party received by the other party that is designated as confidential or proprietary, that the receiving party knew or reasonably should have known was confidential or proprietary, or that derives independent value from not being generally known to the public. Without limiting the generality of the foregoing, Client's Confidential Information shall include Personal Information, and information regarding Client, its customers, sales, marketing, financial information, personnel matters, or means of doing business and projections and marketing strategy; MyWorkplace's Confidential Information shall include its proprietary methodologies and software codes. The confidentiality obligations hereunder will not extend to information that: (i) already known by or available to the receiving party without obligation of confidentiality prior to disclosure under this Agreement; (ii) is or becomes publicly known without breach by the receiving party; (iii) is rightfully received by the receiving party from a third party without a duty of confidentiality; (iv) is independently developed or learned by the receiving party without use of the disclosing Party's Confidential Information; (v) is disclosed by the receiving party with the disclosing party's prior written approval. (vi) is required to be disclosed pursuant to a lawful order of a governmental authority, so long as the Party required to disclose the information provides the Party owning Confidential Information with timely prior notice of such requirement.

c. "**Personal Information**" information that is linked or reasonably linkable to an identified or identifiable individual that is designated by any applicable law or regulation as "personal information" or "personal data" or similar as to any individual who is an employee, officer, agent, shareholder, director or customer of Client.

d. "**Security Breach**" - any actual, probable or reasonably suspected unauthorized access to, or acquisition, use, loss, destruction, compromise or disclosure of, any Client Data, while such information is or was in the possession or control of MyWorkplace or its subprocessors.

2. Processing of Personal Information

a. The processing of any Personal Information by MyWorkplace pursuant to this Agreement shall be: (i) done in accordance with all applicable laws and regulations and solely pursuant to the instructions of Client, (ii) any such personal information shall be treated as Confidential Information and processed as set forth in this Section, (iii) MyWorkplace shall make available

to Client, on reasonable request, all information in MyWorkplace's possession necessary to demonstrate its compliance with the requirements of this Section or applicable law or regulations, (iv) MyWorkplace shall allow, and cooperate with, reasonable data privacy assessments by Client or the Client's designated assessor to the extent required by applicable law or regulation, (v) MyWorkplace shall engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of MyWorkplace with respect to the applicable Personal Information.

3. Responsibility for Data Security.

a. MyWorkplace shall implement and maintain appropriate information and cyber security safeguards ("Safeguards") that prevent the unauthorized access or loss of Client Data, including, without limitation, an information security program that meets the standards of best industry practice to safeguard Personal Information. In addition, MyWorkplace shall store and maintain access to security-related log information from systems, network devices, security solutions, etc. for not less than six (6) months.

b. MyWorkplace agrees to store all Client Data in backup data as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. MyWorkplace further agrees that any and all Client Data stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption.

c. MyWorkplace further agrees that it shall:
   i. Ensure completion of an annual third-party examination of the design and operating effectiveness of MyWorkplace's controls by a reputable certified public accounting firm in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and shall obtain a SSAE 16 Service Organization Control (SOC) 2 report.
   ii. At Client's request, Deliver to Client a full and complete electronic copy of such (SOC) 2 report with an effective date no later than September 30 of each year.
   iii. At Client's request, prepare and deliver to Client a detailed plan for remediating all identified deficiencies and a description of mitigating controls, if applicable, within a reasonable period of time following identification of deficiencies based on the nature and complexity of the deficiencies to be remediated, not to exceed thirty days following identification of such deficiencies; and
   iv. Bear all costs and expenses associated with correcting deficiencies.

3. **Audit Requirements**.

a. Client or an appointed audit firm ("Auditors") shall, once per calendar year at its own costs, have the right to audit the physical and technical environment of MyWorkplace and any applicable subprocessors as it relates to the receipt, maintenance, use, or retention of Client Data, subject to agreement of a standard confidentiality agreement by said Auditors. Client will announce its intent to audit MyWorkplace by providing at a minimum two weeks (10 business days) notice to MyWorkplace. A scope document along with a request for

deliverables will be provided at the time of notification of an audit. If the documentation requested cannot be removed from the MyWorkplace's premises, MyWorkplace will allow the Auditors access to its site.

b. If an adverse opinion on the design and operating effectiveness of MyWorkplace's internal controls is rendered by the independent certified public accounting firm, Client shall, at its option, have the right to terminate the Agreement without additional cost to Client.

4. **Notification**. MyWorkplace shall immediately notify Client of any actual, probable or reasonably suspected Security Breach with respect to Client Data. Immediate notification shall mean as soon as reasonably possible following MyWorkplace's learning of a Security Breach.

5. **Investigation**.

a. MyWorkplace shall (i) assist Client in investigating, remedying and taking any other action Client deems necessary regarding any Security Breach and any dispute, inquiry or claim that concerns the Security Breach; and (ii) shall provide Client with assurance satisfactory to Client that such Security Breach or potential Security Breach will not recur. Unless prohibited by an applicable statute or court order, MyWorkplace shall also notify Client of any third-party legal process relating to any Security Breach, including, but not limited to, any legal process initiated by any governmental entity (foreign or domestic).

b. Client may retain a computer forensics firm to conduct a subsequent investigation if the Client in good faith believes that MyWorkplace did not complete a thorough investigation. Client and any government investigative body and such forensic firm shall be given reasonable access to MyWorkplace's systems and logs with full right to make copies of all such logs which may reasonably relate to the Security Breach. Client and the forensic firms shall enter into a confidentiality agreement with MyWorkplace with respect to any such information derived from MyWorkplace's records and systems.

6. **Breach Notification**.

a. MyWorkplace agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification.

b. MyWorkplace agrees to assume responsibility for informing all such individuals in accordance with applicable law; provided however, that no press release which includes a reference to Client, notification to any Client Related Party or public pronouncement which includes a reference to Client shall be made without Client's prior approval not to be unreasonably withheld or delayed.

8. **Agreement Termination**. Upon written request by Client, MyWorkplace will promptly return or destroy the Client Data, provided that MyWorkplace shall have the right, subject to the requirements of this Agreement, to retain the Client Data to the extent necessary to comply with applicable laws. If so requested by Client, MyWorkplace shall promptly certify to Client that it has complied with this section. If the Client Data is destroyed, at a minimum, a "Clear" media

sanitization is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization, SP800-88.