ACUITY
INFORMATION SECURITY ADDENDUM

This Information Security Addendum ("**ISA**") is made by the parties to the Agreement incorporating this ISA by reference (the "**Agreement**") and governs the obligations of Company to secure all non-publicly available information provided by or on behalf of Acuity to Company ("**Acuity Information**") and all access to any system or software provided by or on behalf of Acuity to Company ("**Acuity Systems**"), in all cases as defined below. This ISA outlines the minimum obligations regarding the subject matter and does not limit either party's responsibility to prevent and respond to security and privacy issues or comply with applicable law.

As used in this ISA:

- **"Acuity"** refers to each of Acuity, Inc. and any Affiliate of Acuity, Inc., but in each chase only when providing access to information or systems covered by this ISA.
- "**Affiliate**" refers to each party any entity that, directly or indirectly, controls, is controlled by, or is under common control with a that party, with "control" meaning holding at least a fifty percent (50%) equity interest of an entity or having the right to direct the disposition of or voting rights of at least fifty percent (50%) of the voting rights of an entity.
- **"Company"** refers to each party to the Agreement other than Acuity, and any Affiliates of that party receiving access to information or systems covered by this ISA.

1. Restricted Access. Company will only grant access to Acuity Information or Acuity Systems where the individual receiving access:

   1.1. Reasonably requires access to perform a legitimate activity that Acuity has expressly authorized the Company to perform, or which a reasonable individual in the industry, with full knowledge of the content of the Acuity Information, would expect the Company to perform in the ordinary course of business and within the scope of the Company's obligations in the Agreement (e.g., system maintenance), while complying with all of the Company's obligations to Acuity; and

   1.2. For each instance of access, has had their identity verified and their use logged through appropriate authentication controls, such as strong passwords, tokens, or biometrics unique to that individual; and

   1.3. When Acuity controls the Acuity Information or Acuity System, the Company will ensure that the individual receiving access does not attempt to circumvent Acuity's access controls (e.g., not sharing passwords, not bypassing identity verification).

2. Security Program. The Company shall maintain a program designed to provide appropriate administrative, technical, and operational measures to secure Acuity Information and Acuity Systems from unauthorized access, use, viewing, modification, copying, and deletion (the "**Security Program**"). The Security Program will comply with all applicable laws, regulations, and industry standards (the "**Laws**"). The Security Program shall include, but is not limited to:

   2.1. Documented policies assigning clear responsibility and authority for activities impacting the security of Acuity Information and Acuity Systems. Examples include acceptable computer use, secure record retention/destruction, asset management, cryptographic controls, access control, environmental and power systems, backups/disaster recovery plans, network security, removable media, remote access, mobile computing, wireless access, change control, segregation of duties, separation of development and production environments, technical architecture management, virus/malware protection, patch

management, media controls, audit logs, time synchronization, network segregation, and system monitoring/logging.

2.2. Documented policies ensuring the Company's collection, use, sharing, disclosure, and protection of any personal or sensitive information in Acuity Information or Acuity Systems comply with the Laws. Upon Acuity's request, the Company shall promptly inform Acuity of all jurisdictions where Acuity Information is stored or processed, or from which Acuity Systems are accessed.

2.3. A process for assessing and monitoring the security of the Company's vendors who have access to Acuity Information and Acuity Systems to ensure compliance with this ISA. The Company agrees that Acuity may hold the Company liable for violations of this ISA by the Company's vendors.

2.4. A process for annual testing and auditing of key controls, systems, policies, and procedures covered by the Security Program to identify and remediate risks, including retaining appropriate documentation of findings.

2.5. A process for annual training of the Company's employees, agents, and contractors regarding their responsibilities under the Security Program.

3. Reviews and Assessments. Acuity or its designated representative shall have the right to monitor, review, and assess the Company's and its vendors' compliance with this ISA. At no cost to Acuity, throughout the term of the relationship the Company agrees to:

3.1. provide the most recent audit reports for any security-related certifications (e.g., SSAE 18, PCI, SOC II, ISO) the Company may have, and a summary of the most recent penetration tests the Company has completed.

3.2. complete questionnaires, provide supporting documentation, and participate in interviews regarding the Company's compliance with this ISA, but only upon Acuity's written request and only if reasonable in scope and length so as to not unreasonably interfere with the Company's business and operations. Unless Acuity reasonably suspects that there has been an Incident, as defined below, or that Company is not complying with this ISA, Acuity will limit its inquiries under this subsection to once in any rolling 12-month period.

4. Public Requests. The Company shall promptly:

4.1. Refer to Acuity any third party inquiries received regarding any obligations to Acuity covered by this ISA.

4.2. Assist Acuity with any requests Acuity receives from individuals related to control over that individual's personal information the Company holds or processes on Acuity's behalf (e.g., requests to disclose, update, delete, export, or restrict the use of that personal information) ("**Acuity DSARs**").

4.3. Refer to Acuity any Acuity DSARs received by the Company.

5. Breach Notification. The Company will provide notice to Acuity of any Incident, as defined below, by sending an email to privacyissues@acuitybrands.com or by calling 844-228-4899 if email is unavailable. Acuity may update this contact information by delivering written notice to the Company.

5.1. For this section, "**Incident**" means any situation where the Company knows of or reasonably suspects, or where a reasonable person with appropriate training and experience in the industry and having completed the due diligence required by this ISA would reasonably suspect:

5.1.1. Loss of control of, unauthorized access to or disclosure of, inappropriate destruction of, or inappropriate use of Acuity Information under the direct or indirect control of the Company, or

5.1.2. Loss of control of or unauthorized access to the Company's or its agent's information or systems which is capable of negatively impacting the security of Acuity Information or Acuity Systems, including facilitating unauthorized access to Acuity Systems or impersonating a representative of the Company in communications with Acuity.

5.2. All notices will include, but only to the best of the Company's knowledge at the time of delivery:

5.2.1. A summary description of the Incident with details adequate to allow Acuity to evaluate the probability the Incident occurred and the risk it may pose to Acuity,

5.2.2. A summary of the Company's response and remediation efforts with details adequate to allow Acuity to evaluate the ongoing risk to Acuity, and

5.2.3. Any other information Acuity may reasonably request to determine its obligations in response to the Incident.

5.3. The Company will provide this notice within a reasonable time after discovering the underlying facts of the Incident, which shall be no longer than seventy-two (72) hours. The Company will also supplement the notice with additional details at least every seventy-two (72) hours (or at such longer intervals as Acuity may authorize in writing) until Acuity has notified the Company in writing that it is satisfied that its interests are protected.

5.4. Unless otherwise required by law, the Company shall not notify any third parties of the Incident's potential impact on Acuity or Acuity's involvement with the Incident unless authorized by Acuity in writing.

6. Suspension and Termination. Upon reasonable suspicion of an Incident or the Company's breach of this ISA, Acuity shall have the right to immediately suspend the Company's access to Acuity Information and Acuity Systems, and Acuity's exercise of this right will neither be considered the basis for Acuity's breach of any of its obligations under the Agreement nor relieve the Company of any of its obligations under the Agreement. If the Company fails to provide Acuity with reasonable comfort that that Acuity Information and Acuity Systems are and have been protected within seven (7) calendar days of suspension, Acuity shall have the right to terminate the Agreement for Company's uncured breach

7. Indemnification. The Company agrees to indemnify Acuity for any violation of this ISA, and no limitation of liability shall apply to the Company's compliance with this ISA.

8. Interpretation. The rights and obligations set forth in this ISA are cumulative with those in the Agreement. Unless expressly and unambiguously stated otherwise in another document signed by both the Company and Acuity, any conflict between this ISA and any other document, including the Agreement, regarding the issues covered by this ISA will be resolved in favor of this ISA. For clarity, to be "expressly and unambiguously stated" for the purposes of the foregoing sentence, there must be a stated intent to override one or more specific provisions of this ISA by explicit and specific reference. General statements regarding document priority or references to "all prior agreements" or "conflicting terms" without specifically identifying both this ISA and the specific terms to be overridden will not be considered adequate.