ACUITY BRANDS
INFORMATION SECURITY ADDENDUM

This Information Security Addendum ("ISA") is made by the parties to the main agreement incorporating this ISA by reference (hereby designated as "Acuity Brands" and "Company", with "Company" applying collectively to all parties to the main agreement other than Acuity Brands). This ISA shall also govern each of the party's Affiliates to the extent that, with respect to Acuity Brands such Affiliates will provide access to information or systems covered by this ISA, and with respect to Company such Affiliates will receive access to information or systems covered by this ISA. "Affiliate" means for 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.

This ISA governs the obligations of Company to secure all non-publicly available information provided by or on behalf of Acuity Brands to Company ("Acuity Brands Information") and all access to any system or software provided by or on behalf of Acuity Brands to Company ("Acuity Brands Systems"). Company agrees to indemnify Acuity Brands for any violation of this ISA and no limitation of liability shall apply to Company's compliance with this ISA. Upon reasonable suspicion of Company's breach of this ISA Acuity Brands shall have the right to immediately suspend Company's right to access Acuity Brands Information and Acuity Brands Systems, and, in addition to any other rights Acuity Brands may have, to terminate Company's performance of activities for Acuity Brands without penalty or further obligation if Company does not cure such breach to Acuity Brands' reasonable satisfaction within seven (7) days of Acuity's written notice. This ISA only states Company's minimum obligations with respect to the subject matter hereof and in no way shall serve as a limit on Company's responsibility to prevent or otherwise respond to security issues or comply with applicable law.

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

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

    1.2. Prior to each instance of access has had their identity verified and their use logged by appropriate application of authentication controls such as strong passwords, tokens, or biometrics that are unique for that individual. For clarity, where Acuity Brands is in control of the Acuity Brands Information or Acuity Brands System it remains Company's obligation to ensure that the individual to whom Company is giving access is not attempting to circumvent the access controls provided by Acuity Brands (e.g., not sharing passwords, not attempting to bypass identity verification).

2. Security Program. At all times Company shall have a program reasonably designed to provide appropriate administrative, technical, and operational measures to secure Acuity Brands Information and Acuity Brands Systems from unauthorized access, use, viewing, modification, copying, and deletion, as applicable (the "Security Program"). In all cases, the Security Program will comply with all laws, regulations, and industry standards applicable to Company, and its access to the Acuity Brands

Information and Acuity Brands Systems (the "Laws"). The Security Program shall include without limitation:

2.1. Documented policies providing clear assignment of responsibility and authority for activities that could impact the security of Acuity Brands Information and Acuity Brands Systems. Potential examples include acceptable computer use, secure record retention/destruction, asset management for both hardware and software, cryptographic controls, physical and technological 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 that the collection, use, sharing, disclosure, and protection of any personal or sensitive information that is in the Acuity Brands Information or contained in the Acuity Brands Systems, as applicable to Company, is performed in compliance with the Laws. Upon Acuity Brands' request, Company shall promptly inform Acuity Brands of all jurisdictions in which Company is storing or processing Acuity Brands Information or from which Company is accessing an Acuity Brands System;

2.3. A process for assessment and ongoing monitoring of the security of Company's vendors who have access to Acuity Brands Information and Acuity Brands Systems to ensure their compliance with the Security Program. Company agrees that Acuity Brands' may hold Company liable for violation of this ISA by Company's vendors;

2.4. A process for at least annual testing and auditing the key controls, systems, policies, and procedures covered by the Security Program to identify and remediate risks, including retention of appropriate documentation showing the findings of such tests and audits; and

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

3. Reviews and Assessments. Acuity Brands or its designated representative shall have the right to monitor, review, and assess Company's and Company's Vendors' compliance with this ISA. At no cost to Acuity Brands, Company agrees to provide the most recent audit reports for any security related certifications (e.g., SSAE 18, PCI, SOC II, and ISO) Company may have and a summary of the most recent penetration tests Company has completed. Additionally, throughout the term of the relationship, when requested by Acuity Brands Company will and at no cost complete questionnaires, provide supporting documentation, and participate in interviews regarding Company's compliance with this ISA, provided that the forgoing is reasonable in scope and length and designed to not unreasonably interfere with Company's business and operations.

4. Data Subject Access Requests. Company shall promptly:

4.1. Refer to Acuity Brands any inquiries received by Company regarding the information security or privacy practices related to Acuity Brands Information or Acuity Brands Systems.

4.2. Assist Acuity Brands with any requests Acuity Brands may receive from individuals related to control over personal information (e.g., requests to disclose what personal information Acuity Brands holds and requests to update, delete, export, or restrict the use of personal information) (collectively "DSARs") included in Acuity Brands Information within Company's control.

4.3. Refer to Acuity Brands any DSARs Company may receive to the extent related to Acuity Brands Information.

5. Breach Notification. Company will notify Acuity Brands of any Incident, as defined below, by sending an email to privacyissues@acuitybrands.com or by calling 844-228-4899 if Company is unable to send email generally. Acuity Brands may update this contact information by delivery of written notice to Company.

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

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

5.1.2. loss of control of or unauthorized access to Company's or its agent's information or systems which a person of appropriate training and experience would believe is reasonably capable of negatively impacting the security of Acuity Brands Information or Acuity Brands Systems, including without limitation by facilitating an unauthorized individual accessing Acuity Brands Systems or impersonating a representative of Company in communications with Acuity Brands.

5.2. To the best of Company's knowledge at the time delivered, the notice will include:

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

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

5.2.3. any other information Acuity Brands may reasonably request to determine Acuity Brands' obligations in response to the Incident.

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

5.4. At any time following receipt of Company's notice, Acuity Brands may suspend Company's right to access Acuity Brands Information and Acuity Brands Systems until such time as Acuity Brands is reasonably satisfied that its interests are protected.

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

6. Interpretation. Unless expressly and unambiguously stated otherwise in another document signed by both Company and Acuity Brands (including any agreement into which this ISA is incorporated), any conflict between this ISA and that agreement with respect to the issues covered by this ISA will be resolved in favor of the terms and conditions of this ISA. For clarity, to be "expressly and unambiguously stated" for the purposes of the forgoing sentence, there must a stated intent to

override one or more specific provisions of this ISA by explicit and specific reference; e.g., 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.