PRIVACY AND DATA PROTECTION APPENDIX

This Appendix applies in the circumstances set out below. In the event of inconsistency or conflict between this Appendix and the Contract Document with respect to a subject covered by this Appendix, the provision requiring the higher level of protection for any Personal Data or other Current information governed by this Appendix shall prevail. The requirements in this Appendix are in addition to any confidentiality obligations between Current and the Supplier under the Contract Document. Current or the applicable Current Affiliate responsible for the protection of any of the Personal Data or other Current information governed by this Appendix may enforce the terms of this Appendix. This Appendix is also applicable when a Supplier affiliate is providing goods, services and/or deliverables under the Contract Document directly, in its own name, in which event Supplier's agreement to the terms of this Appendix is also given on behalf of such Supplier affiliate; and Supplier warrants that it has the power and authority to do so. As used herein, "Supplier" shall mean Supplier and Supplier affiliate, collectively.

SECTION I – DEFINITIONS

The following definitions and rules of interpretation apply in this Appendix. Any words following the terms "including," "include," "e.g.,", "for example" or any similar expression are for illustration purposes only.

(i) ***Contract Document*** means the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of goods, services and/or deliverables by Supplier to Current.

(ii) ***Controlled Data*** is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export controlled data, which is provided by Current to the Third Party in connection with performance of the Contract Document.

(iii) ***EU Law*** means the laws of the European Union or of any member state of the European Union and/or the European Economic Area.

(iv) ***Current*** means Current Lighting Solutions, LLC or a Current Affiliate party to the Contract Document with Supplier.

(v) ***Current Affiliate*** means any entity that is directly or indirectly in control of, controlled by, or under common control with Current, whether now existing, or subsequently created or acquired during the term of the Contract Document.

(vi) ***Current Confidential Information*** is information created, collected, or modified by Current that would pose a risk of causing harm to Current if disclosed or used improperly, and is provided and identified as such to the Supplier under the Contract Document. Current Confidential Information includes Highly Confidential, Personal, Controlled, or Sensitive Personal Data.

(vii) ***Current Highly Confidential Information*** is Current Confidential Information that Current identifies as "highly confidential" in the Contract Document, or that Current identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

(viii) ***Current Information System(s)*** means any systems and/or computers managed by Current, which includes laptops and network devices.

(ix) ***Mobile Devices*** means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

(x) ***Personal Data*** means any information related to an identified or identifiable natural person (Data Subject), as defined under applicable law Processed in connection with the Contract Document. Legal entities are Data Subjects where required by law. Personal Data is Current Confidential Information.

(xi) ***Process(ing)*** means to perform any operation or set of operations upon Current Confidential Information, whether or not by automatic means, including, but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing or destroying.

(xii) ***Security Incident*** means any event in which Current Confidential Information is or is suspected to have been lost, stolen, improperly altered, improperly destroyed, used for a purpose not permitted under the Contract Document or this Appendix, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this Appendix.

(xiii) ***Sensitive Personal Data*** is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance and Portability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special categories of data under applicable law (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation).

(xiv) ***Supplier*** is the entity providing goods, services and/or deliverables to Current pursuant to the Contract Document. Supplier may also be referred to as Third Party.

(xv) ***Supplier Information System(s)*** means any Supplier system(s) and/or computer(s) used to Process, Store, Transmit and/or Access Current Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

(xvi) ***Supplier Personnel*** means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates and third parties (for example, suppliers, contractors, subcontractors, and agents), as well as anyone directly or indirectly employed, engaged or retained by any of them.

(xvii) ***Trusted Third Party Network Connection*** is a physically isolated segment of the Third Party network connected to Current internal network in a manner identical to a standard Current office.

SECTION II – INFORMATION SECURITY REQUIREMENTS. ***This Section II applies whenever a Supplier and/or Supplier Personnel Processes Current Confidential Information, has access to a Current Information System in connection with the Contract Document, or provides certain services to Current. Capitalized terms used in this Section II and not defined in this Appendix shall have the meaning given to them in the Current Third Party Security Requirements referenced herein.***

Part A: Security Controls

Supplier shall comply with the Current Third Party Security Requirements (available at www.led.com/supplier) as applicable to the service, products and/or deliverables provided by the Supplier under the Contract Document, if Supplier will

1. process Current Confidential Information, including hosting applications or providing a cloud computer platform,
2. have access to a Current Information System or a Trusted Third Party Network Connection,
3. develop software for Current,
4. provide data center facility services,
5. support one or multiple critical business functions as defined by Current,
6. high availability requirements or the Third Party's service/application has high availability requirements as defined by Current,
7. leverage virtualization is responsible for the management of the virtual machine image and/or hypervisor, and Processes Current Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data, and/or
8. provide a product that includes executable binary code.

Part B: Security Incidents

1. Supplier shall notify Current without undue delay and no later than within 72 hours after discovery, or sooner if required by applicable law, of any security incident experienced by Supplier in which Current Confidential Information is or is suspected to have been lost, stolen, improperly altered, improperly destroyed, improperly used, or improperly accessed (which includes any Personal Data Breach). Supplier shall report security incidents to Current's Cyber Incident Response Team at current.compliance@currentlighting.com. Supplier shall cooperate with Current in its investigation of an incident, and provide Current a detailed description of the security incident, the type of data that was the subject of the security incident, the identity of each affected person, and any other information Current reasonably requests, as soon as such information can be collected or otherwise becomes available.
2. Unless prohibited by law, Supplier shall provide Current reasonable notice of, and the opportunity to comment on and approve, the content of any notice related to a security incident prior to publication or communication to any third party, except Current shall not have the right to reject content in a security notice that must be included to comply with applicable law.
3. Should Current elect to send a Security Notice regarding a Security Incident, Supplier shall provide reasonable and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.
4. Other than approved Security Notices, or to law enforcement or as otherwise required by law, Supplier may not make any public statements concerning Current's involvement with a Security Incident to any third-party without explicit written authorization of Current's Legal Department.

Part C: Current Audit Rights

1. Current reserves the right to conduct an audit, upon 30 days advance notice, of Supplier's compliance with the requirements in this appendix, including but not limited to: (i) review of the Supplier's applicable policies, processes, and procedures, (ii) review of the results of Supplier's most recent vulnerability assessment and accompanying remediation plans, and (iii) on-site assessments during regular business hours of Supplier's physical security arrangements and Supplier Information Systems. Current reserves the right to conduct an Application Vulnerability Assessment if Supplier's vulnerability assessments do not meet or exceed Current application security requirements. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes Current Confidential Information.

2. Subject to the Confidentiality provisions of the Contract Document, Current or its representative may review, audit, monitor, intercept, access, and disclose any information provided by Supplier that is Processed or stored on Current Information Systems or on Current Mobile Devices accessing the Current network.

Part D: Additional Regulatory Requirements

In the event Supplier Processes Current Confidential Information that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with Current for Current's compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., EU Standard Contractual Clauses, U.S. Protected Health Information Agreement), compliance with additional security requirements, completion of regulatory filings applicable to Supplier, and participation in regulatory audits.

Part E: Supplier Personnel

Supplier is responsible for compliance with this Appendix by all Supplier Personnel. Prior to providing access to any Current Confidential Information to any Supplier Personnel, Supplier must obligate them to comply with applicable requirements of the Contract Document and this Appendix. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel. Supplier may not appoint any third party engaged in providing services and/or deliverables under the Contract Document without the prior written consent of Current. Where such consent has been given, any change of such third party requires Current's prior written approval.

SECTION III – PRIVACY & DATA PROTECTION

Part A. Privacy & Data Protection - General Provisions. ***This Part A applies whenever a Supplier and/or its Supplier Personnel Process Personal Data in connection with the Contract Document.***

1. **Processing**. Supplier will, and will ensure that all of its Supplier Personnel will:
   (a) only Process Personal Data on, and in compliance with, Current's written instructions in a Contract Document and as issued from time to time. Where Supplier believes that any Current instruction violates the terms of the Contract Document or applicable law, unless prohibited from doing so by applicable law, Supplier must inform Current without delay before performing such instruction.
   (b) Process all Personal Data fairly and lawfully and in accordance with all laws applicable to Supplier's activities concerning Personal Data governed by this Appendix; and
   (c) only collect Personal Data directly where Current has provided prior written approval for such direct collection (including where expressly provided in the Contract Document), and, where such direct collection has been approved by Current, comply with applicable data privacy laws and regulations, including provisions concerning notice, consent, access and correction/deletion; any notices to be provided and any consent language to be used when collecting such information directly from a Data Subject are subject to Current's prior and written approval.

2. **International Transfers & Hosting Locations**. Supplier must receive approval from Current prior to (i) moving Personal Data from the hosting jurisdictions identified in the Contract Document to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than such hosting jurisdictions identified in the Contract Document; where Current approves, such approval may be conditioned on execution of additional agreements to facilitate compliance with applicable law.

3. **Inquiries**. Unless prohibited by law, Supplier shall notify Current promptly and act only upon Current's instruction concerning any request by a third party for disclosure of Personal Data or for information concerning Supplier's Processing of Personal Data.

4. **Confidentiality & Information Security**. Supplier shall comply with Section II above if Supplier Processes Personal Data in connection with the Contract Document. Supplier shall limit disclosure of or access to Personal Data to its Supplier Personnel who have legitimate business need-to-know relating to this Contract Document, and who have received proper training and instruction as to the requirements of the Contract Document (such as confidentiality requirements) and this Appendix.

5. **Return of Personal Data and Termination**. Supplier shall, within thirty (30) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of Personal Data and return to Current all copies of Personal Data. In lieu of returning copies, Current may, at its sole discretion, require Supplier to destroy all copies of Personal Data, using agreed upon methods to ensure such Personal Data is not recoverable, and certify to such destruction. Supplier may continue to retain Personal Data beyond the period prescribed in this section above where required by law, or in accordance with the Contract Document and/or applicable regulatory or industry standards, provided that (i) Supplier notifies Current prior to the Contract Document's termination or expiration of the obligation, including the specific reasons for such retention; (ii) Supplier has a documented retention period and secure deletion

procedure for such copies, with back-up copies retained only to the end of their legally required retention period; (iii) following such period, all copies and back-up copies are deleted in such a manner that they are not recoverable; (iv) Supplier performs no Processing of Personal Data other than that necessitated by retaining or deleting the relevant copies; and (v) Supplier continues to comply with all the requirements of this Appendix in relation to any such retained Personal Data until the same is securely deleted. Termination or expiration of the Contract Document for any reason shall not relieve the Supplier from obligations to continue to protect Personal Data in accordance with the terms of the Contract Document and this Appendix.

6. **Supplier Personal Data.** Current may require Supplier to provide certain Personal Data such as the name, address, telephone number, and e-mail address of Supplier's representatives to facilitate the performance of the Contract Document, and Current and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Contract Document, including but not limited to Supplier payment administration. Current will be the Controller of this data for legal purposes and agrees to use reasonable technical and organizational measures to ensure that such information is processed in conformity with applicable data protection laws. Supplier may obtain a copy of the Supplier personal information by written request, or submit updates and corrections by written notice to Current. Current will comply at all times with the privacy policy posted on its web site.

Part B - European Privacy & Data Protection. ***This Part B applies whenever Processing of Personal Data by Supplier and/or Supplier Personnel in connection with the Contract Document falls within the scope of any EU Law or the laws of the United Kingdom. In addition to the other sections of this Appendix, to comply with the requirements of applicable EU law, Supplier agrees to the following (which shall prevail in the event of conflict with the other provisions of this Appendix):***

1. Supplier shall assist Current in the fulfilment of Current's obligations under applicable EU law including
    a. preparation of Privacy Impact Assessments (where required);
    b. response to Data Subject access requests; and
    c. any required breach notification to Data Protection Authorities and Data Subjects.
2. Supplier shall notify Current without undue delay after becoming aware of any Security Incident involving the Processing of Personal Data that falls within the scope of this Part B.
3. Supplier shall assist Current in obtaining approval for Processing from Data Protection Authorities where required.
4. Supplier shall, at Current's election, either return or destroy Personal Data at the termination of the Contract Document (except as required by EU or Member State law).
5. Upon request, Supplier shall provide Current with all information necessary to demonstrate Supplier's compliance with applicable EU law.
6. Where both Current and all Supplier Processing of Personal Data are located within the EU, EEA and/or United Kingdom, or Supplier Processing occurs outside the EU, EEA and/or United Kingdom and related international transfers are subject to a transfer mechanism other than EU Standard Contractual Clauses (e.g. adequacy, Supplier BCR-Processor or EU/Swiss- US Privacy Shield), the categories of Data Subjects' Personal Data Processed and the types of such Personal Data Processed may concern the following:

    Categories of Data Subjects
    Employees; trainees; applicants; contract and temporary workers; directors and others whose personal information is shared with Current in the context of an employment relationship; suppliers; distributors and agents; customers; prospects; and clients.

    Types of Personal Data
    Identification data (name, surname, address, email address, date and other identifying information); professional identification data (CV, professional status, education, awards, job description, hierarchical positioning, performance levels);financial and economic information (bank details, salary); system log data; other personal data that may be contained in business related communications and interactions, internal systems and log data; and sensitive personal data including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, health or medical records and criminal records