UL Solutions Purchase Order Terms

The terms and conditions below ("Terms and Conditions") together with the purchase order (including any incorporated attachments) for Products or Services ("Purchase Order") form an "Agreement" between the UL Solutions Inc. or its Affiliate (each "**UL Solutions**") and the Supplier entity (a "**Supplier**") identified on the Purchase Order. If UL Solutions and Supplier have executed a separate written agreement governing the Products or Services specified in the Purchase Order (the "**Existing Agreement**") then that Existing Agreement will apply to those Products or Services. If these Terms and Conditions conflict with the Purchase Order, the terms of the Purchase Order govern. Any additional or different terms in any Supplier documents, including quotation, acknowledgements, invoices or online terms are void.

1. RETENTION AND DESCRIPTION OF SERVICES. Supplier will perform the services (the "**Services**") and provide the hardware, software, goods, materials, equipment, or other Deliverables (collectively, "**Products**") set forth in each Purchase Order in accordance with the Agreement.

2. AFFILIATES. Under this Agreement, UL Solutions or its Affiliates (an "**Affiliate**" of a party means any other entity that directly or indirectly controls, is controlled by, or is under common control with that party, whether such control exists through voting equity, management control, or by contract) may use the Products and Services procured by UL Solutions or a UL Solutions Affiliate by and for the benefit of any other UL Solutions Affiliate.

3. INVOICING AND PAYMENT.

a. All invoices must include a detailed statement of the Products or Services covered by such invoice and must reference the applicable Purchase Order number. UL Solutions will not be obligated to pay invoices for Products or Services that do not conform to the requirements of this Agreement (including any acceptance criteria). All expenses submitted to UL Solutions for reimbursement must be pre-approved in writing by UL Solutions in accordance with UL Solutions' expense guidelines and charged at actual cost without markup.

b. The price(s) shown on this Purchase Order are firm and may be changed only by a "change order" signed by an authorized UL Solutions. This Purchase Order must not be filled at prices higher than specified or last quoted or charged without UL Solutions' written consent. It is agreed that UL Solutions is to receive the benefit of any decline in price on the material covered by this Purchase Order prior to its execution.

c. UL Solutions will pay Supplier any undisputed invoices within sixty (60) days of receipt of the invoice.

d. UL Solutions' maximum cumulative liability to Supplier in any way related to this Agreement, the Products, or the Services will be equal to the total amount properly invoiced by Supplier in accordance with the terms of this Agreement.

4. CONFIDENTIALITY.

a. Supplier must treat as confidential all documentation or information received from UL Solutions, from a customer of UL Solutions, or from any third party in connection with this Agreement, regardless of the form of receipt, including any documentation or information related to the business, products, or services of UL Solutions or any customer of UL Solutions (collectively, "**Confidential Information**"). "Confidential Information" also includes Work Product (defined below) and any changes, modifications or improvements made by Supplier to any Confidential Information. Supplier may not disclose Confidential Information to any third party or use it for any purpose except as expressly permitted by UL Solutions in writing (which may be in this Agreement). Supplier must immediately return to UL Solutions all Confidential Information (including all copies or materials referring or relating to Confidential Information in its possession or the possession of any third party) as requested by UL Solutions or upon termination or expiration of this Agreement.

b. Confidential Information does not include information that is (i) in the public domain other than due to a violation of this Agreement; (ii) documented to be known to Supplier before disclosure by UL Solutions under this Agreement and without violation of any confidentiality obligation owed to UL Solutions or any third party; or (iii) independently developed by Supplier without reference to or use of Confidential Information. In the event Supplier is required to disclose Confidential Information by law or regulatory authority, Supplier must promptly notify UL Solutions in writing upon receipt of the request and permit UL Solutions a reasonable opportunity to object to or limit the disclosure.

c. This section survives expiration or termination of this Agreement.

5. OWNERSHIP AND INTELLECTUAL PROPERTY RIGHTS. Unless otherwise designated in the Purchase Order, each tangible and intangible deliverable provided by Supplier pursuant to the Agreement and all patent, copyright and other intellectual property rights embodied in or associated with such deliverables (collectively, the "**Work Product**") are "work made for hire" and all right, title, and interest in the Work Product are owned by UL Solutions. If and to the extent any Work Product does not qualify as a "work made for hire," Supplier irrevocably transfers, assigns, and conveys the exclusive ownership to UL Solutions, free and clear of any liens, claims, or other encumbrances, to the fullest extent permitted by law. Supplier will execute and cause its employees, subcontractors, and agents to execute any documents UL Solutions requires to transfer ownership of the Work Product to UL Solutions. Supplier warrants and represents that it will pass good and marketable title to the Work Product, and that the patent, copyright, trademark, trade secret, or other intellectual property interest relating to all Work Product does not infringe, misappropriate, or violate the intellectual property rights of any third party.

6. DATA PRIVACY AND SECURITY.

a. UL Solutions solely owns all right, title, and interest in and to all data and Confidential Information provided to Supplier by or on behalf of UL Solutions, or that Supplier collects under the Agreement (collectively, "**UL Solutions Data**"). Supplier shall have no right, title, or interest in or to any UL Solutions Data. Unless otherwise mutually agreed in an SOW, Supplier shall not sell, retain, use, or disclose UL Solutions Data for any purpose other than performing its obligations under this Agreement.

b. Supplier will implement and maintain technical, physical, and organizational security measures to protect and safeguard UL Solutions Data. Supplier must also comply with the requirements of Exhibit A (Supplier Global Cybersecurity Requirements).

c. In the event that Supplier becomes aware of any actual or suspected (i) breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, UL Solutions Data (ii) unauthorized access, acquisition, disclosure, or use of UL Solutions Data, or (iii) any breach of security with respect to Supplier's (including its subcontractors') systems that store or process UL Solutions Data (in each case, a "Security Incident"), Supplier must (x) provide written notice of the Security Incident to UL Solutions within twenty-four (24) hours; (y) perform an investigation to learn the cause of such Security Incident; and (z) take all steps necessary to remedy the event and prevent reoccurrence. Supplier must cooperate with UL Solutions in the investigation and remediation efforts following a Security Incident and grant UL Solutions access to relevant systems and logs related to said Security Incident.

d. If and to the extent that Supplier processes any UL Solutions Data that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person (collectively, "**Personal Data**"), Supplier will comply with the terms of the Exhibit B (Personal Data Processing Requirements).

e. At the termination or expiration of this Agreement, Supplier must immediately return to all UL Solutions Data. Supplier must immediately destroy all copies of UL Solutions Data collected or processed as part of the services, collected or processed from any UL Solutions system instance(s), or any copies in any computer memory or data storage apparatus. Upon request, Supplier will certify in writing within one week after the termination or expiration of the Agreement that all UL Solutions Data has been either returned or destroyed.

f. This section survives expiration or termination of this Agreement.

7. WARRANTIES.

a. Supplier represents and warrants that: (i) it will use established, sound and professional knowledge, skill, judgment, principles, and practices in accordance with the highest professional and industry standards in its performance of Services; (ii) all Work Product will conform to the specifications, requirements, and descriptions in the Purchase Order; and (iii) it has the right to enter into this Agreement and provide the Products and Services.

b. Product warranties: Supplier represents and warrants that the Products provided by the Supplier to UL Solutions will be a merchantable quality, will conform to applicable specifications, drawings, or descriptions furnished by UL Solutions, will be free from defects in material and workmanship, and will be sufficient and fit for the purposes intended by UL Solutions. UL Solutions' approval of designs, furnished by Supplier shall not relieve Supplier of its obligations under this paragraph. The warranties of Supplier, together with its service guarantees, shall run to UL Solutions and its Affiliates and their subcontractors, dealers, and customers. Supplier shall indemnify and hold UL Solutions and its Affiliates and their employees, customers, subcontractors, and dealers harmless from and against any and all claims, suits, judgments, losses, or expenses, including attorneys' fees, which are grounded or based wholly or partially upon: (i) alleged negligence in the formulation or manufacture of any Products provided by the Supplier to UL Solutions hereunder; or (ii) any alleged defect or actual defect in the Product or upon a claim that the merchandise was not of merchantable quality or that it was not fit for the purpose for which it was intended.

c. Inspection and Acceptance: Receipt or acceptance of all or part of the Products or Services shall not (i) waive UL Solutions' right to cancel or return all or any portion of the Products or Services that do not conform to the Purchase Order; (ii) bind UL Solutions to accept future shipments of Products or Services; or (iii) preclude UL Solutions from making any claim for damages or breach of warranty. All purchases are subject to inspection and rejection by UL Solutions notwithstanding prior payment. Rejected Products will be returned at Supplier's expense for transportation both ways and all related labor and packing costs. No Products returned as defective by UL Solutions shall be replaced by Supplier without written permission of an authorized agent of UL Solutions. UL Solutions may at any time, by written order, make changes within the general scope of this Purchase Order in any one or more of the following: (i) drawings, designs or specifications; (ii) method of shipment or packing; and (iii) place of delivery. If any such change causes an increase or decrease in the cost of, or the time required for, the performance of this Purchase Order, Supplier may request an adjustment in the price or delivery schedule, or both, and the Purchase Order shall be modified in writing accordingly upon agreement by the parties.

8. SHIPPING AND DELIVERY:

a. The Products ordered must be received no later than the delivery date at the location specified by UL Solutions. Supplier will, within twenty-four hours after learning of any cause or condition that would materially delay the delivery of Products, notify the UL Solutions in writing of such anticipated or actual delay, the reasons for such delay, and the actions being taken by Supplier to overcome or minimize the delay. UL Solutions shall be entitled to collect or withhold as liquidated damages an amount equal to a quarter percent (0.25%) of the Purchase Order amount per each day of delay. Such liquidated damages shall not exceed five percent (5%) of the total Purchase Order value per breach. In addition, UL Solutions may terminate any Purchase Order at no charge and without liability as a result of any delay in delivery or poor performance.

b. Any risk of loss associated with the Products rests with the Supplier up to the time of receipt of the Products by UL Solutions at the place of delivery and a proper inspection has been completed by UL Solutions without rejection of the Products. Thereafter, such risk is with UL Solutions including any risk associated with any Products thereafter returned to the Supplier. However, after UL Solutions has returned such Products to the Supplier and the Supplier has received such Products, any risk associated with those Products reverts to the Supplier.

c. Quantities of Products ordered may not be changed without the prior written approval of UL Solutions. If the total or any portion of the Products received either exceeds or falls below the quantities ordered, UL Solutions shall have the right to reject and return any such shipments or portions thereof at Seller's expense for transportation both ways and all related labor and packing costs.

d. Unless otherwise agreed to by both parties, carrier charges for all items to be furnished are to be prepaid. The Products shall be delivered at the expense of the Supplier.

e. No additional charges of any kind, including charges for boxing, packing, cartage, or other extras will be allowed unless specifically agreed to in writing in advance by UL Solutions and unless stated on the front side of this Purchase Order.

f. Products included on this Purchase Order which are of a product category, Listed, Recognized, or Classified by UL Solutions, shall bear the UL Solutions "Listing Mark", "Recognition Mark," or "Classification Mark" specified for the specific category.

9. INDEMNIFICATION.

a. **General Indemnity**. Supplier will defend and hold harmless UL Solutions, and its Affiliates and their respective directors, officers, employees, agents, and contractors ("UL Solutions Indemnitees") from and against any and all causes of action, proceedings, claims, suits, and demands brought by a third party (collectively, "**Claims**") and indemnify the UL Solutions Indemnitees for all damages, losses, penalties, judgments, costs, fines, liabilities, or expenses of whatever nature, (including reasonable legal fees and expenses) (collectively, "**Losses**") that the UL Solutions Indemnitees may incur or suffer arising out of or in connection with the following: (i) Supplier's breach of this Agreement, (ii) actual or alleged personal injury, death, economic loss, or property damage caused by Supplier or its personnel, or (iii) Supplier's gross negligence, willful misconduct, or non-compliance with applicable law.

b. **Intellectual Property Indemnity**. Supplier will defend and hold harmless UL Solutions Indemnitees from and against any and all Claims and indemnify the UL Solutions Indemnitees for all Losses that the UL Solutions Indemnitees may incur or suffer arising out of or in connection with actual or alleged infringement or misappropriation of any patent, copyright, trade secret, or other intellectual property right asserted by any third party (each, an "**IP Infringement Claim**") in connection with any Services, Work Product and Products provided by Supplier under this Agreement. If any Services, Work Product and Products (or any part thereof) becomes, or is likely to become, the subject of an IP Infringement Claim, then Supplier will promptly, using best efforts, at its own expense, and in the order stated: (i) procure for UL Solutions the right to continue using such Services, Work Product, and Products or part thereof, or (ii) replace such Services, Work Product, and Products with a non-infringing product acceptable to UL Solutions, (iii) modify the same so as to make it non-infringing, or (iv) refund to UL Solutions all fees paid for such Services, Work Product, and Products. The forgoing remedies are in addition to any other remedies available to the UL Solutions in equity or at law.

c. This section survives expiration or termination of this Agreement.

10. INSURANCE. Supplier must maintain insurance coverage with appropriate loss limits for this Purchase Order, including any insurance required by the law governing the jurisdiction of Supplier's location or the location where Services are to be performed or Product delivered. Insurance shall be obtained at Supplier's own cost, and containing minimum limits and types as are specified in Exhibit C Supplier will promptly provide evidence of insurance by providing a certificate of insurance. Supplier's certificate of insurance must contain a provision that the coverage afforded under the policy(s) will not be canceled or modified without thirty (30) days prior written notice to UL Solutions. A certificate of insurance must be provided to UL Solutions prior to commencing Services or provision of Products and annually thereafter.

11. COMPLIANCE WITH LAW AND UL SOLUTIONS POLICIES.

a. Supplier must act according to the highest legal, ethical, and moral standards at all times in the performance of Services and provision of Products. Supplier represents and warrants: (i) full and continuing compliance with UL's Supplier Code of Conduct (available at https://www.ul.com/about/ethics-and-compliance) and all applicable tax, anti-bribery, and anti-corruption laws, regulations, and other legal requirements (including the U.S. Foreign Corrupt Practices Act and UK Bribery Act), (ii) no offer, promise, or payment of any money, gift, or any other thing of value will be paid to any person for the purpose of influencing official actions or decisions affecting this Agreement, and (iii) during the term of this Agreement it will not cause UL Solutions to violate any trade sanction laws administered by the U.S. Department of Treasury, U.S. Office of Foreign Asset Control, or other applicable governmental entity, and will obtain all applicable export licenses, and (iv) it will ensure that any payments made to UL Solutions or its Affiliates will not be paid from a financial institution and account subject to any U.S. trade sanction law.

b. Supplier will comply with all applicable laws, regulations, ordinances, and codes including but not limited to, all laws forbidding the solicitation, facilitation, or any other use of slavery or human trafficking.

c. EQUAL OPPORTUNITY; NONDISCRIMINATION, to the extend they apply, the parties shall abide by the requirements of United States Code of Federal Regulations 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a), which prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity or national origin, and require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status or disability.

d. UL Solutions has the right to terminate the Agreement immediately if it is prohibited by applicable law from doing business with Supplier. Supplier agrees to promptly notify UL Solutions of any change in any laws, regulations or other legal requirements that it is aware may affect its performance of this Agreement.

e. If any Supplier personnel enter the premises of UL Solutions or any UL Solutions customer to perform any Services or provide Products, such personnel must: (i) comply with all applicable site policies and (ii) take all required or reasonable precautions to assure their safety and the safety of others. If UL Solutions determines that there has been a breach of the foregoing, UL Solutions may immediately remove such personnel and terminate this Agreement.

12. CONFLICTS OF INTEREST. Supplier may not: (i) use its engagement by UL Solutions for personal financial gain; (ii) accept any personal advantage from anyone under circumstances which might reasonably be interpreted as an attempt to influence the recipients in the conduct of their duties related to this Agreement; or (iii) extend any special favor to employees of UL Solutions under circumstances which might reasonably be interpreted as an attempt to influence them in the conduct of their duties. If Supplier is to conduct assessments, Supplier may not have been involved in any way with designing the product, process, or system to be assessed. If Supplier is an agent authorized by UL Solutions customers, Supplier may not permit any crossover or sharing of information between its personnel who conduct assessments and those who act as agents authorized by UL Solutions customers. Supplier must immediately disclose to UL Solutions any actual or potential conflicts of interest, including any business relationship and/or any financial interest of a UL Solutions employee in Supplier's business.

13. SUBCONTRACTING AND ASSIGNMENT. All Services will be performed and all Products provided by Supplier and its employees. Supplier may not subcontract, assign, or otherwise delegate its obligations under this Agreement except if and as pre-approved by UL Solutions in writing, and in such event, Supplier will be fully responsible for the acts or omissions of such other parties (including with respect to their compliance with this Agreement). UL Solutions may require Supplier to remove or replace any subcontractor(s) or agent(s) whose performance is unacceptable to UL Solutions. In no event shall UL Solutions pay more for subcontracted Services or Products than UL Solutions pays for Supplier's Services or Products (for example, in the case of Services compensated on an hourly basis, time and materials rates for subcontractors shall be the same or less than time and materials rates for Supplier).

14. TERM AND TERMINATION.

a. UL Solutions may terminate this Agreement for any reason, with or without cause, by giving Supplier fifteen (15) days' written notice. During any notice period, Supplier will stop or winddown work in accordance with UL Solutions' instructions. UL Solutions may terminate this Agreement immediately upon notice to Supplier in the event of Supplier's breach of this Agreement, willful misconduct, or gross negligence.

b. Supplier may terminate this Agreement by written notice to UL Solutions in the following circumstances: (i) UL Solutions breaches any material provision of this Agreement and continues of such failure for ten days after written notice, or (ii) UL Solutions becomes insolvent, becomes dissolved or liquidated, or becomes the subject of a petition in bankruptcy, whether voluntary or involuntary, or of any other proceeding under bankruptcy, insolvency, or similar laws; or makes an assignment for the benefit of creditors.

c. Upon Supplier's receipt of a notice of termination from UL Solutions, Supplier will immediately discontinue all Services and provision of Products and will incur no further fees or expenses without UL Solutions' prior written approval. Supplier will reasonably assist UL Solutions in transitioning those Services or provision of those Products to another provider. Further, upon any termination, whether by Supplier or UL Solutions, Supplier will provide UL Solutions all Work Product in process and/or completed through date of termination.

15. INDEPENDENT CONTRACTOR. This Agreement creates only an independent contractor relationship. This Agreement does not create any employment relationship, agency, partnership, or joint venture between the parties. Supplier's personnel performing services under this Agreement will at all times be under Supplier's exclusive direction and control and will not be considered UL Solutions' employees. Supplier will pay all wages, salaries and other amounts due its personnel in connection with Services and provision of the Products and is solely responsible for all obligations respecting their relationship. Supplier, its personnel, and agents are not entitled to any benefits whatsoever (including, without limitation, pension benefits and medical coverage) afforded to UL Solutions' employees. If UL Solutions is required to pay or withhold any taxes or make any other payment with respect to Supplier's personnel or agents, Supplier will reimburse UL Solutions in full for such taxes or payments, and permit UL Solutions to make deductions for taxes required to be withheld from any sum due. Supplier is solely responsible for providing any tools, supplies (except office supplies used on UL Solutions' premises), or other goods that Supplier may need or choose to use in order to perform the Services, except as specifically identified in the Purchase Order.

16. SUPPLIER DIVERSITY. UL Solutions seeks to include Diverse Sellers in awarding bids for goods and services and to identify sellers that will include Diverse Sellers, either directly or indirectly, in servicing the UL Solutions account. "**Diverse Sellers**" include businesses that are owned by minorities, women, LGBTQ+, disabled persons, veterans, as well as those categorized as small businesses. Diverse Sellers must be certified by a national or regional organization that validates diversity status. To support UL Solutions' supplier diversity goal, Supplier will upon request: (a) provide information about its supplier diversity program and good faith efforts to utilize diverse suppliers or subcontractors in its business; (b) submit quarterly reports that identify products and services furnished by Diverse Sellers to Supplier in direct support of the UL Solutions account, if applicable; and (c) document the good faith efforts made during the quarter to increase support of Diverse Sellers, if applicable.

17. ADVERTISING AND PROMOTION. This Agreement does not grant Supplier any rights, authority, or license to use or authorize the use of UL Solutions' marks, name or any abbreviation thereof. Supplier may not use or refer to UL Solutions or its marks in any advertising or promotion without UL Solutions' prior written consent. This section survives expiration or termination of this Agreement.

18. BACKGROUND CHECKS. Supplier will perform background checks of its employees, independent contractors, and other personnel in accordance with applicable law and Supplier's internal policies. Supplier will provide a background check on all Supplier resources who will have access to UL Solutions Data including UL Solutions Confidential Information under the Agreement and who will participate in any way in the provision of Services. Unless otherwise specified in the Purchase Order, the background check will be in accordance with the following specifications and will be done at the Supplier's expense. Supplier will not provide access to Confidential Information or allow participation in any way in the provision of Services or Deliverables for any Supplier resource in the event the background check for such Supplier resource presents any disqualifying findings.

19. Force Majeure. Neither party shall be liable for any failure or delay in the performance of its obligations due to fire, flood, earthquake, elements of nature, acts of God, acts of war, government act, disease, terrorism, system outage (whether due to cyber-attack or other reason outside a party's control), riots, civil disorder, rebellions, or other similar cause beyond the reasonable control of the party affected, provided that such default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented, and, provided further, that the party hindered or delayed immediately notifies the other party describing the circumstances causing the delay.

20. AUDITS AND FINANCIAL RESPONSIBILITY.

a. UL Solutions has the right, upon reasonable notice, to audit during normal business hours Supplier's records pertaining to the performance of this Agreement, regardless of the manner or form in which the Supplier maintains such records. For a period of one year after UL Solutions makes the final payment to Supplier for Supplier's services, UL Solutions may exercise such right as often as UL Solutions deems reasonably necessary and appropriate. UL Solutions may, without penalty, withhold final payment for Supplier's services until such time as UL Solutions' reasonable request to audit Supplier's records is honored. Annually or in the event of a security breach, UL Solutions may (or may engage a third-party auditor to) perform an audit or vulnerability assessment of Supplier's procedures, applications, and IT infrastructure on or through which Supplier or Supplier's subcontractors store, transmit, or accesses UL Solutions Data.

b. If Supplier provides IT or business processing services to UL Solutions, upon UL Solutions' request, Supplier will provide copies of third-party audit reports to UL Solutions at no additional cost. Such audit reports may include Statements of Standards for Attestation Engagements (SSAE #16 Type 2) - SOC 1 for Business Services or SOC 2.

c. If Supplier is a privately held company or subsequently becomes a privately held company, Supplier, on an annual basis, will provide UL Solutions, no later than three (3) months following its fiscal year-end or as soon thereafter as reasonably practicable, its audited financial statements as prepared by or for Supplier in the ordinary course of its business. Financial information provided hereunder will be used by UL Solutions solely for the purpose of determining Supplier's ability to perform its obligations under this Agreement. Any such financial information provided by Supplier to UL Solutions under this section will be treated by UL Solutions as confidential information of Supplier. Supplier agrees to cooperate with sustainability and responsible sourcing audits, and to complete related surveys, within time frames requested by UL Solutions. Failure or refusal of Supplier to respond to any such requests constitutes a material breach of this Agreement.

21. NOTICES. Notices must be in writing and delivered personally, by registered or certified mail, or by email (provided that the sender retains proof of successful time-dated transmission of any email). Notice will be deemed to have been delivered by mail or courier upon the earlier of receipt or five business days after the notice is deposited in the mail or placed with the courier for delivery to a party at the address in the introduction to this Agreement (or at such other address as that party may designate in writing). Notices to UL Solutions must include a copy by email to Legal.Department@ul.com and Supplier's primary contact at UL Solutions.

22. CHOICE OF LAW AND DISPUTE RESOLUTION. All disputes, claims, controversies, questions, or differences related to or arising out of this Agreement will be finally settled by confidential arbitration (except for the limited court remedies provided below). The arbitration will be conducted in English before a single arbitrator agreed to by both parties (or if the parties cannot so agree, an arbitrator appointed by the applicable administrator), in accordance with the then-current rules and procedures of the applicable administrator. The administrator, location, and governing law applicable to the construction and interpretation of this Agreement will be as follows:

a. If UL Solutions' principal place of business is in the United States of America, the arbitration will be administered in Chicago, Illinois by the American Arbitration Association, and the arbitrator will apply the laws of the State of Illinois.

b. If UL Solutions' principal place of business is in Canada, the arbitration will be administered in Toronto by the International Centre for Dispute Resolution Canada, and the arbitrator will apply the laws of Ontario.

c. If UL Solutions' principal place of business is in Latin America, the arbitration will be administered in Miami, Florida, USA by the International Centre for Dispute Resolution, and the arbitrator will apply the laws of the State of Florida.

d. If UL Solutions' principal place of business is in Europe, Africa, or the Middle East, the arbitration will be administered in Zurich, Switzerland by the International Chamber of Commerce, and the arbitrator will apply the laws of Switzerland.

e. If UL Solutions' and Supplier's principal places of business are in China, the arbitration will be administered in Beijing by the China International Economic and Trade Arbitration Commission, and the arbitrator will apply the laws of China. If UL Solutions' principal place of business is in China but Supplier's principal place of business is outside China, the next clause will apply.

f. If UL Solutions' principal place of business is in Asia (except as set forth in the preceding clause), Australia, or New Zealand, the arbitration will be administered in Singapore by the Singapore International Arbitration Centre, and the arbitrator will apply the laws of the Republic of Singapore.

The arbitrator does not have authority to modify this Agreement and must apply the above choice of law without regard to conflicts of law principles. The arbitrator's decision will be the binding and final remedy for any dispute between the parties arising out of this Agreement. However, a party may seek from a court of competent jurisdiction: judgement on an arbitration award, provisional remedies in aid of arbitration, or injunctive relief to stop a breach or threatened breach of this Agreement.

23. MISCELLANEOUS.

a. This Agreement, its exhibits, and any documents incorporated by reference constitutes the parties' entire agreement and understanding and supersedes any prior communications, understandings, representations, negotiations, and discussions (written or oral) between the parties regarding the subjects of this Agreement. No terms or conditions on either party's purchase orders, quotations, invoices, or other business forms will apply to any transaction under this Agreement. Any modification to this Agreement must be in writing and signed by both parties.

b. The headings appearing in this Agreement are included only for convenience and in no way define or limit the scope or intent of any portion of this Agreement. Terms defined in the plural include the singular and vice versa.

c. The rights and remedies of the parties are cumulative and not exclusive and are in addition to any other rights and remedies the parties may have under law. Any failure by a party to insist upon the performance of any provision of this Agreement will not constitute a waiver of any rights under the Agreement or future performance of that provision.

d. No provisions of this Agreement in any way inure to the benefit of any third party other than UL Solutions' Affiliates, and the parties intend that no such third party will have any claim under this Agreement.

e. If any provision in this Agreement or in any instrument or document delivered pursuant to this Agreement is invalid, illegal, or unenforceable, the validity, legality and enforceability of the remaining provisions will not be affected or impaired.

f. This section survives expiration or termination of this Agreement.

Exhibit A

Supplier Global Cybersecurity Requirements

1. **Purpose**

1.1. This Supplier Global Cybersecurity Requirements document describes the minimum cybersecurity requirements that Supplier shall comply with in performing services for, or otherwise accessing data belonging to, the contracting entity or entities including their Affiliates (the "UL Solutions") under the applicable service agreements, statements of work, or any other related documents (collectively, "Agreements"). All capitalized terms not defined herein shall have the meaning set forth in the Agreements.

2. **Global Cybersecurity Management Program**

2.1. Supplier shall have an Information Security Management Program ("ISMP") that addresses the overall security program of Supplier. The ISMP shall be formally documented, and such records shall be protected, controlled, and retained according to applicable international, federal, state, or internal requirements.

2.2. Supplier management support for the ISMP shall be demonstrated through signed acceptance or approval by management.

2.3. UL Solutions shall have the right to assess the effectiveness of the ISMP by reviewing Supplier's information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management support at least annually.

3. **Access Control**

3.1. Access Control Policy. Supplier shall establish, document, and, upon UL Solutions' request, communicate to UL Solutions, a formal access control policy based on business and security requirements for access. Access control rules shall account for and reflect Supplier's policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users shall be clearly stated. Access controls must be both logical and physical. Users and service providers shall be given a clear statement of the business requirements to be met by access controls. The policy shall be reviewed and updated at least annually.

3.2. Review of User Access Rights. All access rights shall be regularly reviewed by management through a formal documented process.

3.2.1. **User Registration**. Supplier shall implement and document a user registration and de-registration procedure for granting and revoking access. User account types shall be identified and conditions for group and role membership shall be established.

3.2.2. **User Identification and Authentication**. Supplier shall require users to have unique identifiers (user IDs) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of the user. Supplier shall provide a list of all user accounts that will have access to UL Solutions Confidential Information on an as needed basis. Authentication and authorization mechanisms shall be applied for users and equipment.

3.2.3 **User Attestation**. Supplier shall perform, at least bi-annually, an all-user attestation process. The User Attestation process is an ongoing review and confirmation of user access that will correlate users with their access to systems and applications, evaluate risk associate with required access and deem user access as risky or inappropriate.

3.2.4. **Privilege Management**. Supplier shall restrict and control the allocation and use of privileges to information systems and services through a formal authorization process. Privileges shall be allocated to users on a need-to-use basis and on least privileges in line with the access control policy.

3.3. **Secure Log-on Procedures**. Supplier shall control user access to operating systems with secure log-on procedures that will display general notice warnings that computers may: (i) only be accessed by authorized accounts; (ii) limit the number of unsuccessful log-on attempts; (iii) enforce recording of unsuccessful attempts; (iv) force time delay before further log-on attempts are allowed; (v) reject any further attempts without specific authorization from an administrator; and (vi) not display the password being entered by hiding the password characters and symbols.

3.3.1. Password Management. Supplier shall ensure that passwords are controlled through a formal management process. Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of strong passwords.

3.3.2. User Authentication for External Connections. Supplier shall develop and implement appropriate authentication methods to control access of remote users to systems containing UL Solutions Confidential Information by requiring the use of password or passphrase and at least one (1) of the following: a cryptographic-based technique, biometric techniques, hardware tokens, software tokens, a challenge/response protocol, or certificate agents.

3.4. Network Services and Connection Control. Supplier shall specify the networks and network services to which users are authorized to access. Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. The capability to connect to shared networks shall be restricted in line with the access control policy and requirements of the business applications.

3.4.1. Equipment Identification in Networks. Supplier shall use automatic equipment identification as a means to authenticate connections from specific locations and equipment to determine whether or not they are permitted to connect to the Supplier's network.

3.4.2. Remote Diagnostic & Configuration Port-Protection. Supplier shall control the physical and logical access to diagnostic and configuration ports. Controls for the access to diagnostic and configuration ports shall include the use of a key lock. Ports, services,

and similar applications installed on a computer or network systems, which are not specifically required for business functionality, shall be disabled or removed.

3.4.3. Segregation in Networks. Groups of information services, users, and information systems shall be segregated on networks. Supplier shall implement and maintain security gateways which include but are not limited to firewalls and intrusion detection or protection systems which will forward event data and security alerts to a centralized SEIM system for analysis, reporting, and incident response. Supplier shall perform firewall configuration and Access Control List reviews on a regular basis, but not less often than monthly, to ensure appropriate controls and configurations are applied to limit traffic to only what is required for business operations, shall be used between internal network, external networks, and any demilitarized zone (DMZ).

3.4.4. Network Protection. Supplier shall implement and maintain firewalls and intrusion detection or protection systems which will forward event data and security alerts to a centralized SEIM system for analysis, reporting, and incident response. Supplier shall perform firewall configuration and Access Control List reviews on a regular basis, but not less often than monthly, to ensure appropriate controls and configurations are applied to limit traffic to only what is required for business operations.

4. Human Resources Security

4.1. Roles & Responsibilities. Supplier shall define and document the security roles and responsibilities of employees, contractors, and third-party users in accordance with Supplier's information security policy. Supplier shall ensure that workforce members agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to Supplier's assets associated with information systems and services.

4.2. Terms and Conditions of Employment. Supplier shall ensure that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to UL Solutions' assets associated with information systems and services.

4.2.1. Screening. Supplier shall conduct background verification checks on all candidates for employment, contractors, and third-party users in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

4.2.2. Disciplinary Process. A formal sanctions process shall be established and implemented for employees who have violated security policies and procedures.

4.2.3. Removal of Access Rights. The access rights of all employees, contractors, and third-party users to information and information assets shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment. Changes of employment or other workforce arrangement shall be reflected in removal of all access rights that were not approved for the new employment or workforce arrangement.

4.3. Information Security Awareness, Education, and Training. Supplier shall ensure that all employees, contractors, and third-party users receive appropriate awareness training and regular updates in Supplier's policies and procedures, as relevant to their job function.

5. Risk Management

5.1. Risk Management Program. Supplier shall create and implement a comprehensive program that manages the risks to information system operations, assets, and UL Solutions Confidential Information. The risk management program shall develop means through which the Supplier shall manage and mitigate risks to UL Solutions, including physical and environmental hazards.

5.2. Risk Assessments. Supplier shall perform risk assessments to identify and quantify information security risks to UL Solutions. Supplier shall account for risks from sources including prior incidents experienced, changes in the environment, and any supervisory guidance. Risk assessments are to be performed at least annually, or when major changes occur in the environment, and the results reviewed annually.

6. Information Security Policy

6.1. Information Security Policy. Supplier shall develop, publish, and implement information security policy documents. The information security policy shall state the purpose and scope of the policy, communicate management's commitment, describe management's and workforce member's roles and responsibilities, and establish Supplier's approach to managing information security. The documents shall be reviewed at planned intervals or if significant changes occur to ensure the policies' adequacy and effectiveness.

7. Organization of Information Security

7.1. Confidentiality Agreements. Supplier shall ensure that all personnel who access to UL Solutions Confidential Information have agreed to confidentiality or non-disclosure restrictions.

7.2. Independent Review of Information Security. Supplier shall review at least annually, or when significant changes to the security implementation occur, Supplier's approach to managing information security and its control objectives, controls, policies, processes, and procedures. The review shall include an assessment of Supplier's adherence to its security plan, address the need for changes to the approach to security in light of evolving circumstances, and be carried out by individuals independent of the area under review who have the appropriate skills and experience.

7.3. Information Security Framework. Supplier shall follow a leading, industry recognized cyber security framework, e.g., National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO) 27001. Each year, Supplier shall complete UL Solutions' supplier cybersecurity assessment questionnaire. If Supplier fails to satisfy UL Solutions' supplier security assessment in UL Solutions' sole opinion, UL Solutions may terminate any relevant SOW by giving Supplier fifteen (15) days' prior written notice.

7.3.1. Regulatory Audits and Examinations. To the extent permitted by law, Supplier shall notify UL Solutions if an international, federal or state regulatory agency requests a review, audit, or other examination of the services or records maintained by Supplier on behalf of UL Solutions. Supplier shall fully cooperate with UL Solutions and any regulator(s) in the event of an audit or review.

7.4. Identification of Risks Related to Third Parties. Supplier shall identify the risks to its information and information assets from business processes involving third parties and then implement appropriate security controls. Supplier shall evaluate any information security risks posed by third parties prior to establishing a relationship with such third party. Once a relationship has been established, Supplier shall evaluate the third party's information systems on a scheduled ongoing basis.

7.4.1. Addressing Security in Third Party Agreements. Supplier shall ensure that agreements with third parties involving accessing, processing, communicating or managing its information or information assets, or adding products or services to information assets cover all relevant security requirements. Supplier shall identify and mandate information security controls to specifically address third party access to its information assets. Supplier shall maintain written agreements with its third parties that include an acknowledgement that such third parties are responsible for the security of the information.

7.5. Evidence of Third-Party Risk Management Program. For Suppliers that maintain or retain data and provide access to any third party, Supplier shall provide evidence of a third-party risk management program. Upon request from UL Solutions, Supplier agrees to provide evidence of an assessment of any third parties that have access to UL Solutions' data.

8. Compliance

8.1. Identification of Applicable Legislation. Supplier shall explicitly define, document, and maintain all relevant statutory, regulatory, and contractual requirements for each information system type. The specific controls and individual responsibilities to meet these requirements shall be similarly defined and documented and then communicated to the user community through a documented security training and awareness program.

8.2. Protection of UL Solutions Records. Supplier shall protect important records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

8.3. Regulation of Cryptographic Controls. Supplier shall use cryptographic controls in compliance with all relevant agreements, laws, and regulations. Supplier shall implement strong cryptographic controls for secure file transfers, data at rest, and email communications, etc. which may contain sensitive data. The compliance with all relevant regulations shall be reviewed at minimum on an annual basis.

8.4. Information Systems Audit Controls. Supplier shall develop audit requirements and activities involving checks on operational systems to minimize the risk of disruptions to business processes. An annual audit planning and scoping process shall exist and consider risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit.

8.5. Payment Card Industry Information Security Standard Requirements. To the extent Supplier receives, accesses, or transmits cardholder data (e.g., credit or debit card data), Supplier acknowledges its responsibility to secure cardholder data and agrees to comply with applicable Payment Card Industry Information Security Standard requirements.

9. Asset Management

9.1. Inventory and Acceptable Use of Assets. Supplier shall identify and create an inventory of assets and information. All information systems shall be documented and include rules for acceptable use and a method to accurately identify and assign ownership responsibilities to the proper individuals. The rules for acceptable use shall be communicated to all information system users and describe their responsibilities and expected behavior with regard to information and information system usage.

9.2. Classification Guidelines. Supplier shall implement and maintain a process to classify information based on its relevant legal requirements, sensitivity, and its criticality to Supplier so that limitations can be put on the data internally and externally. Appropriate procedures for information labeling and handling shall be developed based on the classification system adopted by the Supplier.

9.3. Information Labeling and Handling. Supplier shall implement and maintain an appropriate set of procedures for information labeling and handling in accordance with the classification scheme adopted by Supplier. Sensitive information shall be physically and/or electronically labeled and handled appropriately regarding the level of risk the information or document contains.

10. Physical and Environmental Security

10.1. Physical Security Perimeter. Supplier shall protect areas that contain information and information assets with security perimeters (barriers such as walls, card-controlled entry gates, or manned reception desks). These areas shall not be located in areas that are unattended or have unrestricted access by the public.

10.2. Physical Entry Controls. Supplier shall protect secure areas with appropriate entry controls to ensure only authorized personnel are allowed access. Supplier shall maintain visitor access logs for facilities where information systems reside.

10.2.1. Working in Secure Areas. Supplier shall design and apply physical protection and guidelines for working in secure areas. The arrangements for working in secure areas shall include controls for the employees, contractors, and third-party users.

10.2.2. Public Access Areas. Supplier shall control access points, such as delivery and loading areas, and other points where unauthorized persons may enter the premises and, if possible, isolate them from information processing facilities to avoid unauthorized access.

10.3. Securing Offices, Rooms, and Facilities. Supplier shall design and apply physical security for offices, rooms, and facilities to restrict access from the public.

10.4. Equipment Siting. Supplier shall site or protect equipment to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.

10.4.1. Supporting Utilities. Supplier shall protect equipment from power failures and other disruptions caused by failures in support utilities. Support utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning, shall be regularly inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

10.5. Cabling Security. Supplier shall protect power and telecommunications cabling carrying data or supporting information services from interception or damage. Clearly identifiable cable and equipment markings shall be used to minimize handling errors and access to patch panels and cable rooms shall be controlled.

10.6. Equipment Maintenance. Supplier shall correctly maintain equipment to ensure its continued availability and integrity by developing, communicating, and reviewing / updating a formal, documented information system maintenance policy and procedures.

10.7. Secure Disposal or Re-Use of Equipment. Supplier shall check all items of equipment containing storage media to ensure that UL Solutions Confidential Information and licensed software has been removed or securely overwritten prior to disposal. Surplus equipment shall be stored securely while not in use. Devices containing UL Solutions Confidential Information shall be physically destroyed or the information shall be destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. Certificate of destruction is required to be provided by Supplier upon deletion of UL Solutions Confidential Information.

10.8. Removal of Property. Supplier shall ensure that equipment, information, or software shall not be taken off site without prior authorization and documentation. Employees, contractors, and third-party users who have authority to permit off-site removal of assets shall be clearly identified.

11. Communications and Operations Management

11.1. Documented Operations Procedures. Supplier shall formally document and maintain operating procedures and make them available to all users who need them. The documented procedures shall be prepared for system activities associated with information and communication assets.

11.2. Change Management. Supplier shall control and archive changes to information assets, systems, networks, and network services. Formal change management responsibilities and procedures shall be in place to ensure satisfactory control of all changes.

11.3. Segregation of Duties. Supplier shall enforce the separation of duties to reduce opportunities for unauthorized or unintentional modification or misuse of Supplier's assets. No single user shall be able to access, modify, or use assets without authorization or detection. Supplier shall identify duties that require separation and define information system access authorizations to support separation of duties.

11.4. Separation of Development, Test, and Operational Environments. Supplier shall separate and control development, test, and operational environments to reduce the risks of unauthorized access or changes to the operational system.

11.5. Monitoring and Review of Third-Party Services. Supplier shall regularly monitor and review the services, reports, and records provided by third parties. Audits shall be carried out regularly to govern and maintain compliance with the service delivery requirements.

11.5.1. Managing Changes to Third Party Services. Supplier shall ensure that third parties use appropriate change management procedures for any changes to their provision of services or internal system. Changes to the provision of services, including maintaining and improving existing information security policies, procedures, and controls shall be managed, taking account of the criticality of business systems and processes involved and reassessment of risks.

11.6. System Acceptance. Supplier shall establish acceptance criteria for new information systems, upgrades, and new versions. Suitable tests of the systems shall be carried out during development and prior to acceptance to maintain security. Management shall ensure that requirements for acceptance of new systems are clearly defined, agreed upon, and documented.

11.7. Controls Against Malicious Code. Supplier shall implement detection, prevention, and recovery controls to protect against malicious code, and also provide appropriate user awareness procedures. Formal policies shall be required, and technologies implemented for the timely installation and upgrade of the protective measures, including the installation and regular, automatic updating of anti-virus or anti-spyware software, including anti-virus definitions, and additional end point security controls should be implemented, such as windows firewall, and Data Loss Prevention solution, etc., and to be current whenever updates are available. Periodic reviews/scans shall be required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software.

11.8. Back-up. Supplier shall create and regularly test back-up copies of information and software and store them in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site. A formal definition of the level of back-up required for each system shall be defined and documented including the scope of data being imaged, frequency of imaging, and duration of retention. This document shall be based on the contractual, legal, regulatory, and business requirements.

11.9. **Network Controls**. Supplier shall manage and control networks in order to protect UL Solutions from threats and to maintain security for the network, including information in transit. Supplier shall implement controls to ensure the security of information in networks and the protection of connected services from unauthorized access. Controls shall be implemented to ensure the availability of network services and information services using the network. Responsibilities and procedures shall be established for the management of equipment on the network, including equipment in user areas.

11.10. **Management of Removable Media**. Supplier shall document and implement formal procedures for the management of removable media. Media containing UL Solutions Confidential Information shall be physically stored and its data encrypted in accordance with the Supplier's data protection and privacy policy on the use of cryptographic controls until the media is destroyed or sanitized, and commensurate with the confidentiality and integrity requirements for its data classification level.

11.10.1. Physical Media in Transit. Supplier shall protect media containing UL Solutions Confidential Information against unauthorized access, misuse, or corruption during transportation beyond Supplier's physical boundaries.

11.11. Exchange Agreements. Supplier shall establish and implement agreements for the exchange of information and software between Supplier and its third parties. The agreements shall specify the minimum set of controls on responsibility, procedures, technical standards, and solutions.

11.12. Audit Logging. Supplier shall produce audit logs recording user activities, exceptions, and information security events and keep them for an agreed period to assist in future investigations and access control monitoring. Retention for audit logs shall be specified by Supplier and retained accordingly.

11.13. Protection of Log Information. Supplier shall protect logging systems and log information against tampering and unauthorized access. Access to system audit tools and audit trails shall be limited to those with a job-related need.

11.14. Monitoring System Use. Supplier shall establish procedures for monitoring use of information processing systems and facilities to check for use and effectiveness of implemented controls. The result of the monitoring activities shall be reviewed periodically. Supplier shall comply with all relevant legal requirements applicable to its monitoring activities. Items that shall be monitored include authorized access and unauthorized access attempts.

11.15. Clock Synchronization. Supplier shall ensure that the clocks of all relevant information processing systems within the Supplier's environment have been synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines.

12. Information Systems Acquisition, Development and Maintenance

12.1. Input Data Validation. Supplier shall apply checks to the input of business transactions, standing data, parameter tables, and information into applications and databases when system development is being performed to ensure that data is correct and appropriate.

12.2. Output Data Validation. Supplier shall validate data output from an application to ensure that the processing of stored information is correct and appropriate to the circumstances. Output validation shall be manually or automatically performed when system development on applications and database is being conducted.

12.3. Policy on the Use of Cryptographic Controls. Supplier shall develop and implement a policy on the use of cryptographic controls and support it with formal procedures. The cryptographic policy shall be aligned with the Supplier's data protection and privacy policy and shall address the use of encryption for protection of information transported by mobile or removable media, devices, or across communication lines.

12.4. Key Management. Supplier shall support the use of cryptographic techniques with the practice of key management. All cryptographic keys shall be protected against modification, loss, and destruction. Secret and private keys shall require protection against unauthorized disclosure, and all cryptographic keys shall be limited to the fewest number of custodians necessary. Equipment used to generate, store, and archive keys shall be physically protected, and encryption keys shall be stored separately from encrypted data.

12.5. Protection of System Test Data. Supplier shall carefully select, protect and control test data in non-production environments. The use of operational databases containing UL Solutions Confidential Information for non-production purposes shall be avoided. UL Solutions Confidential Information must not be used for testing purposes.

12.6. Access Control to Program Source Code. Supplier shall restrict access to program source code and associated items to prevent the introduction of unauthorized functionality and avoid unintentional changes.

12.7. Outsourced Software Development. Supplier shall supervise and monitor outsourced software development. Supplier shall have a contract for the outsourced development in place with the third party and address licensing arrangements, certification of the quality and accuracy of the work carried out, rights of access for audit of the quality and security functionality of code.

12.8. Control of Technical Vulnerabilities and Penetration Testing. Supplier shall perform vulnerability scans at intervals consistent with industry best practices to identify potential technical vulnerabilities based on notification of ZERO day vulnerabilities. Supplier shall subscribe to industry recognized threat monitoring service. Once a potential technical vulnerability has been identified, Supplier shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls. Supplier shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required. Supplier shall agree in writing that prior to production the application will undergo vulnerability and source code analysis. Postproduction, Supplier shall perform contractually agreed upon security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase. Supplier shall provide written documentation to UL Solutions of the results of the scans and tests along with a mitigation plan. Supplier shall agree in writing that these vulnerabilities shall be mitigated pursuant to the policies of each Customer entity.

13. Information Security Incident Management

13.1. Reporting Information Security Incidents. Supplier shall report Security Incidents through appropriate communications channels in accordance with the Agreements. All employees, contractors, and third-party users shall be made aware of their responsibility to report any Security Incidents as quickly as possible. Formal Security Incidents reporting procedures to support Supplier's corporate policy shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of a Security Incident, treating the breach as discovered, and the timelines of reporting and response. Supplier standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.

13.2. Responsibilities and Procedures. Supplier shall establish management responsibilities and procedures to ensure a quick, effective, and orderly response to Security Incidents.

13.3. Incident Response Plan. Supplier shall be able to implement and maintain an existing incident response plan containing milestones and service level-agreements for its incident response capability, describing the structure and organization of the incident response capability, providing a high-level approach for how the incident response capability aligns with its overall organizational policies and procedures, and meets the unique requirements of the Supplier, which relate to mission, size, structure, and functions. The incident response plan will also define reportable

incidents and resources needed to effectively maintain and mature an incident response capability, as well as provide metrics for measuring the incident response capability. The plan shall then be approved by designated Supplier officials.

13.3.1. Copies of the incident response plan shall be distributed to incident response personnel and Supplier organization elements.

13.3.2. Reviews of the incident response plan shall occur annually and include a table-top exercise, documentation, test plan, and results.

13.3.3. Revisions to the incident response plan shall be made to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

13.3.4. Supplier shall communicate incident response plan changes to incident response personnel and organizational elements.

13.4. Collection of Evidence. Supplier shall collect, retain, and present evidence after a Security Incident. The evidence that is collected, retained, and presented shall be done in accordance with the laws of the relevant jurisdiction(s).

14. Disaster Recovery Plan and Business Continuity Management

14.1. Including Information Security in the Disaster Recovery Plan and Business Continuity Management Process. Supplier shall develop and maintain a managed program and process to maintain or restore operations and ensure availability of information, at the required level and in the required time frames following interruption to, or failure of, critical business processes for business continuity. Supplier shall maintain a single framework of business continuity plans to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. The program and process shall identify all the assets involved in critical business practices, consider the purchase of suitable insurance, ensure the safety of personnel and the protection of information assets, formulate and document business continuity plans, and address information security requirements in line with the agreed upon business continuity strategy. Supplier must provide results of Business Continuity Planning (BCP) sessions on an at least annual basis. BCP exercises must be conducted and reviewed with all downstream suppliers. Supplier will document BCP processes and procedures in support of products and services provided. This includes plans for the loss of critical resources including workplace, work force, third-party suppliers, and applications.

14.2. Testing, Maintaining, and Re-Assessing Business Continuity Plans. Supplier shall test and annually update business continuity plans to ensure that they are up to date and effective. The business continuity plan tests shall ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

Exhibit B

Personal Data Processing Requirements

If Supplier accesses, handles, uses, stores, transmits, or otherwise Processes Personal Data as part of its provision of Services for UL Solutions, the following terms apply.

1) Definitions.

   a) "**Controller**" means the entity, alone or jointly with others, that determines the purposes and means of the Processing of Personal Data. For the avoidance of doubt, also known as, "Personal Information Processor" under the PIPL.

   b) "**Data Subject**" means an identified or identifiable natural person.

   c) "**Data Protection Legislation**" means the applicable laws or regulations, or decisions, codes of practice and guidance of a competent institution supervising or regulating data protection, in each case, relating to the Processing of Personal Data and privacy; including where applicable, (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR") and national data protection laws in the European Union ("EU") and European Economic Area ("EEA"), and the data protection laws of Switzerland and of the United Kingdom (including the Privacy and Electronic Communications (EC Directive) Regulations 2003, UK Data Protection Act 2018 and the UK GDPR) (collectively "European Data Protection Laws") , (ii) the People's Republic of China ("PRC") Personal Information Protection Law, and its implementing regulations and measures ("PIPL"), and/or (iii) the California Consumer Privacy Act (Cal. Civ. Code 1798.100-1798.199) ("CCPA"), in each case, as may be amended from time to time.

   d) "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. "Personal Data" includes personal information and personal data (as those terms are defined in the applicable Data Protection Legislation), as context requires.

   e) "**Process**", "**Processed**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

   f) "**Processor**" the entity that Processes Personal Data on behalf of the Controller. For the avoidance of doubt, also known as a party, entrusted by a Personal Information Processor under PIPL.

   g) "**Standard Contractual Clauses**" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914.

2) **Authority.**

   a) UL Solutions authorizes Supplier to Process the Personal Data during the term of the Agreement as a Processor (on its and its Affiliates behalf) only for the purposes of providing the Services. Personal Data may include information of UL Solutions employees/contractors maintained for employment purposes and professional contact and other business information of UL Solutions' clients and partners, as applicable under the Agreement.

   b) Schedule 1 hereto describes the purposes of the parties' Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.

   c) Schedule 1 lists the parties' statuses under relevant Data Protection Legislation.

   d) The subject matter and duration of the Processing, the nature and purpose of the Processing, and the type of Personal Data and categories of Data Subjects may be more specifically described in a statement of work, UL Solutions purchase order, or written agreement signed by the parties' authorized representatives, which forms an integral part of the Agreement; if this is the case, the more specific description will control over Schedule 1.

3) **Supplier Obligations.** Supplier will (and will procure that any Authorized Sub-Processor will):

   a) Process Personal Data only on documented instructions from UL Solutions, including the Agreement. Supplier will immediately inform the controller if, in its opinion, an instruction infringes the Data Protection Legislation or other data protection provisions;

   b) will Process Personal Data only to the extent required to provide the Services;

   c) not Process Personal Data for any purpose other than for the business purposes specified in Agreement or otherwise retain, use or disclose Personal Data outside of the direct business relationship between UL Solutions and Supplier.

   d) not permit any Processing of Personal Data of (i) subject to European Data Protection laws outside the European Economic Area, Switzerland and/or the United Kingdom, or (ii) Chinese residents outside the PRC, in each case, without UL Solutions prior written consent which may be subject to conditions at UL Solutions' discretion (unless Supplier or Authorized Sub-Processors are required to transfer the Personal Data, to comply with applicable laws and such laws prohibit notice to UL Solutions on public interest grounds);

   e) ensure that any person authorized to process the Personal Data: (a) have committed themselves to appropriate contractual confidentiality obligations or are under an appropriate statutory obligation of confidentiality; (b) Processes the Personal Data solely on behalf and in accordance with the instructions from UL Solutions; and (c) are appropriately reliable, qualified, and trained in relation to their Processing of Personal Data;

f) implement (and assist UL Solutions to implement) technical and organizational measures to ensure a level of security appropriate to the risk presented by Processing the Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed, and comply with the UL Solutions Supplier Minimum Security Requirements set forth in Exhibit A to the Agreement;

g) in the event that Supplier becomes aware of any actual or suspected (i) breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data (ii) unauthorized access, acquisition, disclosure, or use of Personal Data, or (iii) any breach of security with respect to Supplier's (including its subcontractors') systems that store or process Personal Data (in each case, a "Security Incident"), Supplier must (x) provide written notice of the Security Incident to UL Solutions within twenty-four (24) hours; (y) perform an investigation to learn the cause of such Security Incident; and (z) take all steps necessary to remedy the event and prevent reoccurrence. Supplier must cooperate with UL Solutions in the investigation and remediation efforts following a Security Incident and grant UL Solutions access to relevant systems and logs related to said Security Incident;

h) provide reasonable assistance to UL Solutions in: (a) responding to requests for exercising the rights of Data Subjects under applicable Data Protection Legislation, including by deleting Personal Data, correcting Personal Data, disclosing the specific pieces of Personal Data Processed by the Supplier, insofar as this is possible; (b) reporting any Security Incident to any supervisory authority or Data Subjects and documenting any Security Incidents; (c) taking measure to address Security Incidents, including, where appropriate, measures to mitigate its possible adverse effects; (d) conducting privacy and data protection impact assessments (and personal information protection impact assessment, if applicable) of any Processing operations and in consulting with any applicable supervisory authority or appropriate persons accordingly and (e) undertaking any other activities which may be necessary or requested by UL Solutions for compliance with the Data Protection Legislation; and

i) securely delete or return all Personal Data to UL Solutions (at the choice of UL Solutions) after the end of the provision of services relating to processing in accordance with the Agreement.

4) **Sub-processing.** Supplier will not engage, use or permit any third party (including Supplier's Affiliates) to Process Personal Data without the prior written consent of UL Solutions, which may be withheld or subject to conditions at UL Solutions' discretion. If UL Solutions has consented to the use of third parties (subsequently, an "**Authorized Sub-Processor**") for the Processing of Personal Data: (i) Supplier will provide UL Solutions with advance notice of any intended changes to any Authorized Sub-Processor, allowing UL Solutions sufficient opportunity to object and (ii) the Authorized Sub-Processor's activities must be specified and the same contractual terms set out in this Exhibit must be imposed on that Authorized Sub-Processor. Without prejudice to subsection (i) above, Supplier will remain responsible for all acts or omissions of the Authorized Sub-Processor as if they were its own.

5) **Compliance with Data Protection Legislation.**

a) Supplier will comply with applicable Data Protection Legislation, and will not cause UL Solutions to breach any obligation under the Data Protection Legislation. Supplier will notify UL Solutions without undue delay, if in the delivery of the Services as an experienced supplier of the Services, it identifies any potential areas of actual or potential non-compliance with the Data Protection Legislation. Supplier will comply with any additional legal requirements that are necessary to address issues related to compliance with applicable Data Protection Legislation.

b) Some jurisdictions require that an entity transferring Personal Data to a recipient take extra measures to ensure that the Personal Data has special protections if the law of the recipient's jurisdiction does not protect Personal Data in a manner equivalent to the transferring entity's jurisdiction (an "International Data Transfer Mechanism"). The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Legislation, including the Standard Contractual Clauses. If the International Data Transfer Mechanism on which the parties rely is amended, invalidated or superseded, the parties will work together in good faith to find a suitable alternative. With respect to Personal Data of Data Subjects located in a jurisdiction that requires an International Data Transfer Mechanism, (e.g., the EEA, Switzerland, or the United Kingdom) or Personal Data otherwise subject to European Data Protection Laws that UL Solutions transfers to Supplier or permits Supplier to access, the parties agree that by executing this Agreement they also execute the Standard Contractual Clauses, which will be incorporated by reference and form an integral part of this Agreement, and be considered duly executed and completed upon entering into force of this Agreement. The parties agree that the parties will comply with the provisions of the applicable Module of the Standard Contractual Clauses specified in Schedule 1 and, with respect to the elements of the Standard Contractual Clauses that require the parties' input, Schedules 1 and 2 contain information relevant to the Standard Contractual Clauses' Annexes. In case of any conflicts or inconsistency between the provisions of this Agreement and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail. The parties agree that, for Personal Data of Data Subjects in the United Kingdom, Switzerland, or another country specified in Schedule 1, they adopt the modifications to the Standard Contractual Clauses listed in Schedule 1 to adapt the Standard Contractual Clauses to local law, as applicable. Supplier further agrees that Supplier has conducted a data transfer impact assessment in accordance with Clause 14 of the Standard Contractual Clauses and Supplier agrees to provide UL Solutions with that documentation upon request and/or continue to cooperate with UL Solutions in ensuring compliance with the Standard Contractual Clauses and relevant legal obligations. If so required by applicable Data Protection Legislation or regulatory procedures of any jurisdiction, the Parties will execute or re-execute the Standard Contractual Clauses as separate document setting out the proposed transfers of Personal Data in such a manner as may be required.

c) Without limiting the generality of the foregoing, Supplier will enter into (and will cause its subcontractors or sub-processors to enter into) any additional agreements or adhere to any additional contractual terms and conditions related to the Processing, including cross border data transfer, of Personal Data as UL Solutions may instruct in writing that UL Solutions deems necessary to comply with Data Protection Legislation.

6) **Additional CCPA Compliance**. Without limiting the foregoing, Supplier shall not (i) sell or otherwise make available Personal Data to a third-party for monetary or other valuable consideration, or (ii) share or otherwise make available Personal Data to a third-party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration. In addition, Supplier shall not combine Personal Data that Supplier receives from, or on behalf of, UL Solutions with personal information that Supplier receives from, or on behalf of, another person or persons, or collects from its own interaction with the Data Subject, provided that the Supplier may combine personal information to perform any business purpose as permitted by CCPA.

7) **Information and audit provision**. Supplier will make available to UL Solutions all information necessary to demonstrate compliance with the obligations set forth in this Exhibit and allow for and contribute to audits, including inspections, conducted by UL Solutions or another auditor mandated by UL Solutions. UL Solutions will provide reasonable advance notice (where feasible) of any such audit. UL Solutions shall perform such audit during regular business hours and in such a manner that does not interfere with normal business activities.

Schedule 1: Description of the Transfer and Processing

Table 1: UL Solutions Enterprise Employee Data

Subject Matter of Processing Activity	**Status of the Parties**	**Categories of Data Subjects**	**Categories of Personal Data that May Be Processed** *The categories listed are descriptive and do not necessarily mean that the parties are processing each category of data listed.*	**Categories of Sensitive Data that May Be Processed** *The categories listed are descriptive and do not necessarily mean that the parties are processing each category of data listed.*	**Applicable Module of the Standard Contractual Clauses**
Supplier Processes Personal Data to provide the Services.	Data exporter: UL Solutions is a Controller. Data importer: Supplier is a Processor. If UL Solutions acts as a Processor to another Controller, UL Solutions is a Processor and Supplier is a Sub-Processor	Past, present and future staff of the data exporter, including volunteers, trainees, agents, interns, contractors, temporary and casual workers ("employees")	Name; date of birth; address; telephone number; email address; education and employment details such as employment history, training, professional skills, assignments, individual development plans, performance goals and assessment, performance, attendance, employment status; nationality; details of immigration status Financial details such as bank account numbers (IBAN or other applicable information), social security number, social fiscal number or other national identification number Name, date of birth and contact details of spouses, dependents and emergency contacts Any information UL Solutions employees may choose to share with other UL Solutions employees through the group wide communication and processing tools (such as Outlook, Lync, SharePoint, Yammer).	Health information about employees, as relevant for their employment with the data exporter, including provision of benefits such as health insurance (if applicable), workplace safety management, and leave/absence management. An employee could voluntarily disclose religion or sexual orientation information as part of the benefits or leave management process, though UL Solutions does not ask for this information	Module 2 Module 3, if UL Solutions acts as a Processor to another Controller

Table 2: UL Solutions **Enterprise Business Customer Data**

Subject Matter of Processing Activity	**Status of the Parties**	**Categories of Data Subjects**	**Categories of Personal Data that May Be Processed** *The categories listed are descriptive and do not necessarily mean that the parties are processing each category of data listed.*	**Categories of Sensitive Data that May Be Processed** *The categories listed are descriptive and do not necessarily mean that the parties are processing each*	**Applicable Module of the Standard Contractual Clauses**

				category of data listed.	
Supplier Processes Personal Data to provide the Services.	Data exporter: UL Solutions is a Controller. Data importer: Supplier is a Processor. If UL Solutions acts as a Processor to another Controller, UL Solutions is a Processor and Supplier is a Sub-Processor	Present and future business customers of the data exporter, including employees and contact persons of customers and business partners ("business customers")	Name; professional email address; company; job title; work location; departments; business address; professional telephone number (including mobile telephone number) Purchase and transaction history (where applicable), including bank account information used for payment. Device and/or activity Data related to interactions with UL's hardware and software. Location data IP address Device preferences & personalization Service usage for websites, webpage click tracking. Metadata and telemetry Payment instrument data Device IDs Diagnostic Data Log Data	None	Module 2 Module 3, if UL Solutions acts as a Processor to another Controller

Information for International Transfers

Categories of data subjects whose personal data is transferred.

See Table 1 and Table 2 of Schedule 1.

Categories of personal data transferred.

See Table 1 and Table 2 of Schedule 1.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Table 1 and Table 2 of Schedule 1.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data is transferred on a continuous basis during the term of the Service Agreement, unless otherwise specifically agreed elsewhere between UL Solutions and Supplier.

Nature of the processing

Supplier will Process Personal Data as necessary to perform the Services pursuant to the Service Agreement as further instructed by UL Solutions and/or its UL Solutions Affiliates or subsidiaries by virtue of using the Services, including storage, organization, structuring, disclosure by transmission, dissemination or making available, and other forms of processing.

Purpose(s) of the data transfer and further processing

The Purpose of the data transfer and processing by Supplier is to provide the Services to UL Solutions and, as applicable, its UL Solutions Affiliates, as further specified in the Service Agreement and other Supplier Contracts (if any).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

As a Processor, Supplier retains Personal Data it collects or receives from the UL Solutions Enterprise for the duration of the Service Agreement and consistent with its obligations under applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

Supplier uses the Subprocessors listed in a statement of work or written agreement signed by the parties' authorized representatives when it acts as a Processor. Supplier will engage sub-processors solely as necessary to provide the Services to UL Solutions and, as applicable, its UL Solutions Affiliates, and sub-processors will carry out any processing of personal data only as necessary for such purposes and as further instructed by UL Solutions and/or its UL Solutions Affiliates by virtue of using the Services, including hosting, storage and other forms of processing. Such processing will be no longer than for the duration of the Service Agreement, unless otherwise agreed upon in writing.

For the purposes of the Standard Contractual Clauses:

- Clause 9(a) (Module 2 and 3, as applicable): The parties select Option 2. The time period is 30 days.
- Clause 11(a): The parties do not select the independent dispute resolution option.
- Clause 17: The parties select Option 1. The parties agree that the governing jurisdiction is Ireland.
- Clause 18: The parties agree that the forum is Ireland.
- Annex I(A): The data exporter is UL Solutions (defined above), and the data importer is the Supplier (defined above).
- Annex I(B): The parties agree that Schedule 1 describes the transfer.
- Annex I(C): The competent supervisory authority is the Irish Data Protection Commission.
- Annex II: The parties agree that Schedule 2 describes the technical and organizational measures applicable to the transfer.

For the purpose of localizing the Standard Contractual Clauses:

- Switzerland
    - Any references to the GDPR, the EU or EU Member State law in the Standard Contractual Clauses shall have the same meaning as the equivalent reference in Swiss data protection laws. To the extent a transfer is also subject to the GDPR, the parties adopt the GDPR standard for all data transfers.
    - Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Swiss Federal Data Protection and Information Commissioner (insofar as the transfer is governed by Swiss data protection laws) and, concurrently (where the transfer is also subject to the GDPR), the EEA member state authority identified above.
    - Clause 17: The parties agree that the governing jurisdiction is Ireland.
    - Clause 18: The parties agree that the forum is Ireland. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).

- The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.

- United Kingdom
  - For the purposes of transfers of personal data from the UK, the Parties agree to comply with the terms of Part 2: Mandatory Clauses of the Addendum, being the template UK International Data Transfer Addendum B.1.0 issued by the UK Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses. The Parties also agree that the information included in Part 1 of the Addendum shall be as set out above. The parties also agree that the Exporter and Importer may end the Addendum as set out in Section 19 of the Addendum.
  - The parties agree that the Standard Contractual Clauses are deemed amended to the extent necessary that they operate for transfers from the United Kingdom to a Third Country and provide appropriate safeguards for transfers according to Article 46 of the United Kingdom General Data Protection Regulation ("*UK GDPR*"). Such amendments include changing references to the GDPR to the UK GDPR and changing references to EU Member States to the United Kingdom.
  - Clause 17: The parties agree that the governing jurisdiction is the United Kingdom.
  - Clause 18: The parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.

Schedule 2: Technical and Organizational Security Measures

Supplier will comply with the Supplier Global Cybersecurity Requirements set forth in Exhibit A to the Agreement.

Exhibit C

Insurance Requirements

During the term of this Agreement, Supplier must procure and maintain, at its sole expense, insurance covering its activities at the project premises. Such insurance must be secured from a company(s) authorized to conduct business in the territory in which work is to be performed, and from insurers with an A.M. Best rating of no less than A:VII (or equivalent financial strength rating for similar agency in Supplier's jurisdiction) unless otherwise agreed by UL Solutions. Such insurance must be at least as broad as set forth below for the applicable type of Services, unless otherwise agreed within the Existing Agreement which may supersede such requirements.

Proof of Insurance: Supplier shall provide a Certificate of Insurance from insurer(s) prior to commencing work for UL Solutions. Prior to the expiration of policies, a renewal Certificate of Insurance shall be provided to UL Solutions until such time that the contract is terminated. Each insurance policy required above shall provide that coverage shall not be canceled, except with prior written notice to UL Solutions. Insurance Certificates should be delivered to: globalsuppliermaintenance@ul.com or as otherwise directed by UL Solutions.

General minimum insurance requirements by region are provided below. UL Solutions reserves the right to adjust insurance requirements subject to the scope of work. Additionally, any statutory insurance required in Supplier's local jurisdiction must be maintained to be in compliance with local laws and regulations.

United States of America	**Commercial General Liability Insurance** 1.1. Limits of no less than USD $1,000,000 each occurrence and USD $2,000,000 General Aggregate. 1.2. If Supplier will be conducting any work on UL Solutions premises, an endorsement adding UL Solutions, its Affiliates, and their trustees, directors, officers, and employees, as Additional Insureds is required. **Automobile Liability (required if transportation services are provided or supplier is operating vehicles on UL** Solutions **premises)** 2.1. Limits of no less than USD $1,000,000 for Bodily Injury Liability and Property Damage, covering owned, leased, hired, and non-owned vehicles. 2.2 If Supplier will be performing services on UL Solutions premises or transporting any goods or people on behalf of UL Solutions, Supplier will cause UL Solutions to be included as an additional insured under Supplier's automobile liability policy. **Workers' Compensation** 3.1. as required by statute in the jurisdiction where work is to be performed and Employers Liability insurance with a limit of no less than USD $1,000,000 per accident for bodily injury or disease. 3.1. If Supplier will be conducting any work on UL Solutions premises, a Waiver of Subrogation in favor of UL Solutions is required, to the extent permitted by law. **Professional Liability / Errors & Omissions** (required if Supplier is providing professional services of any kind) 4.1. Limits of no less than USD $5,000,000 per claim and in the annual aggregate. **Cyber Liability insurance** (required if Supplier will have access to Personally Identifiable Information (PII), Personal Health Information (PHI), or Intellectual Property of UL Solutions or UL Solutions' clients (IP).) 5.1. Limits of no less than USD $3,000,000 each claim and in the annual aggregate.
Canada	**Commercial General Liability Insurance** 1.1. Limits of no less than CDN $1,000,000 each occurrence and CDN $2,000,000 General Aggregate. 1.2. If Supplier will be conducting any work on UL Solutions premises, an endorsement adding UL Solutions, its Affiliates, and their trustees, directors, officers, and employees, as Additional Insureds is required. **Automobile Liability (required if transportation services are provided or supplier is operating vehicles on UL Solutions premises)** 2.1. Limits of no less than CDN $1,000,000 for Bodily Injury Liability and $500,000 for Property Damage, covering owned, leased, hired, and non-owned vehicles. 2.2 If Supplier will be performing services on UL Solutions premises or transporting any goods or people on behalf of UL Solutions, Supplier will cause UL Solutions to be included as an additional insured under Supplier's automobile liability policy. **Professional Liability / Errors & Omissions** (required if Supplier is providing professional services of any kind) 4.1. Limits of no less than CDN $5,000,000 per claim and in the annual aggregate. **Cyber Liability insurance** (required if Supplier will have access to Personally Identifiable Information (PII), Personal Health Information (PHI), or Intellectual Property of UL Solutions or UL Solutions' clients (IP).) 5.1. Limits of no less than CDN $3,000,000 each claim and in the annual aggregate.
Latin America	**Commercial General Liability Insurance** 1.1. Limits of no less than USD $500,000 (or **local currency** equivalent)each occurrence and USD $500,000 (or **local currency** equivalent) General Aggregate. 1.2. If Supplier will be conducting any work on UL Solutions premises, an endorsement adding UL Solutions, its Affiliates, and their trustees, directors, officers, and employees, as Additional Insureds is required.

	Automobile Liability (required if transportation services are provided or supplier is operating vehicles on UL Solutions premises) 2.1. Limits of no less than USD $500,000 (or **local currency** equivalent) for Bodily Injury Liability and Property Damage, covering owned, leased, hired, and non-owned vehicles. 2.2 If Supplier will be performing services on UL Solutions premises or transporting any goods or people on behalf of UL Solutions, Supplier will cause UL Solutions to be included as an additional insured under Supplier's automobile liability policy. **Workers' Compensation and Employers Liability** 3.1. as required by statute in the jurisdiction where work is to be performed **Professional Liability / Errors & Omissions** (required if Supplier is providing professional services of any kind) 4.1. Limits of no less than USD $500,000 (or **local currency** equivalent) per claim and in the annual aggregate. **Cyber Liability insurance** (required if Supplier will have access to Personally Identifiable Information (PII), Personal Health Information (PHI), or Intellectual Property of UL Solutions or UL Solutions' clients (IP).) 5.1. Limits of no less than USD $500,000 (or **local currency** equivalent) each claim and in the annual aggregate.
Europe, Australia, or New Zealand	**Commercial General Liability Insurance (Public Liability Insurance)** 1.1. Limits of no less than EUR 1,000,000 each occurrence (or **local currency** equivalent) and EUR 2,000,000 (or **local currency** equivalent) General Aggregate. **Automobile Liability (required if transportation services are provided or supplier is operating vehicles on UL** Solutions **premises)** 2.1. Limits of no less than EUR 1,000,000 (or **local currency** equivalent) for Bodily Injury Liability and Property Damage, covering owned, leased, hired, and non-owned vehicles. **Workers' Compensation & Employers Liability** 3.1. as required by statute in the jurisdiction where work is to be performed **Professional Liability / Errors & Omissions** (required if Supplier is providing professional services of any kind) 4.1. Limits of no less than EUR 5,000,000 (or **local currency** equivalent) per claim and in the annual aggregate. **Cyber Liability insurance** (required if Supplier will have access to Personally Identifiable Information (PII), Personal Health Information (PHI), or Intellectual Property of UL Solutions or UL Solutions' clients (IP).) 5.1. Limits of no less than EUR 3,000,000 (or **local currency** equivalent) each claim and in the annual aggregate.
Africa or the Middle East	**Commercial General Liability Insurance (Public Liability Insurance)** 1.1. Limits of no less than USD 250,000 (or **local currency** equivalent) each occurrence and USD 250,000 (or **local currency** equivalent) General Aggregate. **Automobile Liability (required if transportation services are provided or supplier is operating vehicles on UL** Solutions **premises)** 2.1. Limits of no less than USD 250,000 (or **local currency** equivalent)for Bodily Injury Liability and Property Damage, covering owned, leased, hired, and non-owned vehicles. **Workers' Compensation & Employers Liability** 3.1. as required by statute in the jurisdiction where work is to be performed **Professional Liability / Errors & Omissions** (required if Supplier is providing professional services of any kind) 4.1. Limits of no less than USD 1,000,000 (or **local currency** equivalent) per claim and in the annual aggregate.
China	**Commercial General Liability Insurance (Public Liability Insurance)** 1.1. Limits of no less than RMB 5,000,000 (or **local currency** equivalent) each occurrence and RMB 5,000,000 General Aggregate. **Employers Liability** 2.1. in accordance with and meeting all requirements of applicable law and not less RMB 200,000 (or **local currency** equivalent) for each employee **Professional Liability / Errors & Omissions** (required if Supplier is providing professional services of any kind including engineering, architect, or laboratory testing services) 3.1. Limits of no less than RMB 2,000,000 (or **local currency** equivalent) per claim and in the annual aggregate.