lightenUp

LIGHTENUP AI SERVICES LTD.

lightenUp AI Services | | hello@lightenup.ai

The contract is ready for review and signature. If you have any questions, just ask!

Hyperflow AI Services contract

1. Services

1.1 Ordering Services. Supplier will provide the Services described in this Agreement and in any Service Order in accordance with the terms and conditions of this Agreement and the applicable Service Order. Each Service Order will become a part of and be governed by the terms of this Agreement. Any inconsistency between any provisions of this Agreement and the provisions of a Service Order will be resolved in favor of this Agreement, unless the applicable Service Order explicitly states otherwise. The Parties agree that time is of the essence for initiating the Implementation Services (as "Implementation Services" are defined in Section 1.3 below) and for commencing the Services. Supplier will promptly notify the Customer of any delay or anticipated delay in the performance of the Implementation Services and/or the Services, the reasons for the delay(s) and the actions being taken by Supplier to overcome or mitigate the delay(s). Any Affiliate may enter into Service Orders with Supplier under this Agreement, and with respect to such Service Orders, such Affiliate becomes a party to this Agreement and references to the Customer in this Agreement are deemed to be references to such Affiliate.

1.2 Hosted Services. Supplier will provide the Hosted Services to the Customer and make the System accessible to the Customer in order for the Customer and its users to access, use and receive the Hosted Services as described in a Service Order. Supplier will provide the Customer with the Support and Maintenance Services described in Exhibit B, and will (a) provide the Customer with all assistance required in connection with the proper use of the Hosted Services and System, and (b) test and maintain the System and Hosted Services and ensure that each is accessible for use by the Customer and its Affiliates and operates effectively and reliably. Supplier will provide the Hosted Services and System in accordance with the performance standards set forth in the applicable Service Order and Exhibit C attached hereto.

1.3 Implementation Services. If set forth in a Service Order, Supplier will configure and implement the System and Services pursuant to specifications to be mutually agreed upon in writing by the Parties ("Implementation Services"). Supplier will own any and all improvements to the System made by or on behalf of Supplier that arise out of the Implementation Services including those improvements based on the Customer's requirements for the System and Services as communicated by the Customer to the Supplier, (the "Customer Requirements") particularly extending to any logic or system architectures developed by Supplier. This provision specifically safeguards the Intellectual Property rights of Supplier with respect to such innovations to the System and Services, which will remain exclusively owned by Supplier. In addition, all written reports, requirements documents, specifications, program materials, flow charts, notes, outlines and the like that are developed, conceived or made by Supplier in connection with Supplier's performance of the Implementation Services that are derived from, based on or contain any the Customer Requirements (collectively, "Written Deliverables") shall be the exclusive property of Supplier.

1.4 Professional Services. Supplier will provide the Customer with any Professional Services that are described in a Service Order.

1.4.1 Work Product, Proprietary Rights and Pre-Existing Work. Unless otherwise clearly specified in a Service Order, where Supplier delivers or is required to deliver to the Customer any Work Product in connection with any Professional Services under a Service Order, then the Supplier shall remain the sole and exclusive property of the Work Product, including all intellectual property rights therein, save for exceptions delineated below. The Supplier asserts that such Work Product is not a "work made for hire" for copyright purposes, and all copyrights in the Work Product are retained by the Supplier. In the event that the Work Product encompasses material subject to copyright, patent, trade secret, or any proprietary rights protection, the Supplier does not assign but reserves all right, title, and interest therein. The aforementioned reservation of rights includes any inventions, designs, and intellectual property rights embodied in the Work Product or created during the Supplier's development of the Work Product. This includes a license under any current and future patents owned or licensable by the Supplier, necessary for the Customer to utilise the Work Product in combination with any of their products, services, offerings, software, or intellectual property.

1.4.2 Suggestions and Feedback. If the Customer provides any Suggestions or Feedback to Supplier, Supplier will be entitled to use the Suggestions without restriction. The Customer hereby irrevocably assigns to Supplier all right, title, and interest in and to the Suggestions. The Customer acknowledges Supplier's right to use it without further notice or any compensatory obligations towards the Customer.

2. Payment

2.1 Fees. For timely and professional delivery of the Services and for all rights granted herein in connection therewith, the Customer agrees to pay Supplier the fees as set forth in the Service Order (the "Service Fees"). Under no circumstances may Supplier include on its invoices any fees and/or charges unless the Parties have either specifically agreed to such fees and/or charges in the applicable Service Order, or have otherwise agreed to such fees and/or charges in writing in advance (including but not limited to fees and/or charges arising out of or related to researching, reporting on or correcting tax, accounting or reconciling errors or shortfalls). Supplier will, in accordance with generally accepted accounting standards, keep copies of all books and records relating to the Services during the term of this Agreement and for three (3) years thereafter.

2.2 Invoicing. Supplier will submit invoices to the Customer for payment as set forth in the applicable Service Order. Such invoices shall clearly itemize all Services (along with any deliverables and/or results) provided and the amount billed for the same. For example, if an invoice includes amounts specifically pertaining to contract Implementation Services, Supplier shall call those out on the relevant invoice(s) with specificity (i.e., on an itemized basis). Payment of undisputed amounts due hereunder will be made by the Customer to Supplier within thirty (30) days after the Customer's receipt and validation of properly submitted and correct invoice(s). If any invoice is disputed, the disputed amount will be due and payable within thirty (30) days after resolution of such dispute. If Supplier does not invoice the Customer for Services (or expenses that the Customer has agreed to reimburse, in writing and in advance) within twelve (12) months after performing such Services or incurring such expenses, Supplier hereby waives all right to payment or reimbursement by the Customer.

2.3 Late Payment. If the Customer fails to make payment within the thirty (30) day period as stated in Section 2.2, and provided that Supplier has sent the Customer a payment reminder and the payment remains due after fourteen (14) days of receipt of such reminder, the provision of Services will not be interrupted at this stage. If the overdue payment is not received by Supplier within thirty (30) days from the original due date, Supplier reserves the right to interrupt the provision of the Services until the outstanding payment is fully settled. Notwithstanding the interruption of the Services, the outstanding payment remains due, and the interest shall accrue on the overdue amount at a rate of 9% per annum, or the maximum rate permitted by law, whichever is lower, from the due date until the date of actual payment. The right to interrupt the Services is in addition to, and not instead of, Supplier's other rights under this Agreement and applicable law.

2.4 Taxes.

2.4.1 Notwithstanding anything to the contrary in a Service Order, all Service Fees are exclusive of any sales, use, excise, value added tax, or any other tax or amount (collectively "Taxes"). In the event that Supplier is legally obligated to charge the Customer for any applicable Taxes, Supplier shall ensure that Supplier's original invoice (a) itemizes each such Tax, (b) complies with all applicable regulations governing the issuance of tax invoices, and (c) includes a detailed description of the Services and/or Deliverables giving rise to such Taxes.

2.4.2 Notwithstanding Section 2.4.1, if the Customer provides the Supplier with a tax exemption certificate authorized by the appropriate taxing authority, the Supplier shall not invoice, and the Customer shall have no obligation to pay the Taxes covered by such certificate.

3. Use of the Services

3.1 System. Supplier hereby grants to the Customer during the Service Order Term (as defined in the applicable Service Order), a non-exclusive, worldwide, royalty-free, fully paid-up, non transferable (except on assignment of the Agreement) license to access and use the System for the purposes of using and receiving Hosted Services. the Customer may sublicense the foregoing rights to any third parties who perform services for the Customer as necessary for such third parties to perform services for the Customer.

3.2 The Customer shall:

(a) comply with all applicable laws and regulations with respect to its activities under this Agreement;

(b) not use the Services intentionally to create harmful content, meaning any material intended to cause considerable harm to the Customer itself or to third parties, or to disseminate misinformation;

(c) not use the Services to produce content intended to be deceitfully represented as human-generated;

(d) not use the Services to create content that would be regarded by a reasonable person as sexually explicit or excessively violent;

(e) not use the Services in a way that infringes upon or violates the rights of others, including, but not limited to, illicitly obtaining personal information;

(f) not engage in activities aimed at disabling, disrupting, or otherwise compromising the security of the Services, including but not limited to efforts to circumvent or disable any content moderation or safety measures put in place by Supplier;

(g) not utilize the Services to reverse engineer, decompile, or otherwise attempt to acquire the underlying models, algorithms, or source code of the Services, or to develop competitive products;

and (h) not engage in scraping, "crawling", or "spidering" any pages, data, or portions of the Services, whether this be performed manually or through automated means.

3.3 The Customer's Account. For the provision of certain Services delineated in the applicable Service Order, access to an Account will be necessary. This Account will be under the sole control and responsibility of the Customer. Except to the extent caused by Supplier's act or omission or the act or omission of any of Supplier's Affiliates or any third party engaged by Supplier,

(a) the Customer is responsible for all activities that occur under its Account, regardless of whether the activities are authorized by the Customer or undertaken by the Customer, the Customer's employees or a third party (including your contractors, agents or End Users),

and (b) Supplier is not responsible for unauthorized access to the Customer's Account.

(c) The provision of the credentials and specific access permissions to the Account will be specified in the applicable Service Order that contemplates the provision of any Service requiring access to an Account. Supplier shall provide to the Customer all credentials and documentation necessary for such access, and shall deal promptly with any issues raised by the Customer in respect of its access to or use of the Account.

4. Confidentiality, Privacy and Security

4.1 The Customer Data.

4.1.1 Access. Supplier shall ensure that the Customer has unrestricted and immediate access to, and the right to review and retain, all Customer Data within the Supplier's control or otherwise held by the Supplier. Customer Data includes all files containing data and information originating from the Customer's operations, services, or activities and also data generated or derived from the analysis, processing, or use of such data.

4.1.2 Restrictions. The Supplier may collect, use, store, and retain Customer Data only where expressly authorized under the applicable Service Order and solely as necessary to perform the Services in accordance with this Agreement and that Service Order.

4.2 Confidentiality; Customer Information.

4.2.1 Confidentiality. The receiving Party of any Confidential Information from the disclosing Party agrees to use the Confidential Information solely for the purposes provided by the disclosing Party, not to disclose the Confidential Information to any third party, and to protect the Confidential Information from unauthorized use and disclosure. The Customer may share Confidential Information with its Affiliates. The Supplier may disclose Confidential Information only to employees, professional advisors, and subcontractors on a need-to-know basis, provided they comply with these confidentiality obligations, or if required by any judicial or governmental request, requirement, or order, with reasonable prior notice to the disclosing Party to contest the disclosure. The obligations of this section do not apply to information that becomes publicly available through no fault of the receiving Party, is obtained from a third party not in connection with this Agreement, is independently developed by the receiving Party, is disclosed with the prior written consent of the disclosing Party, or is required by applicable law. The Supplier shall not issue any publicity, advertising, press release, or public statement regarding this Agreement or use the Customer's name or trademarks without prior written approval from the Customer. This section shall survive termination of this Agreement.

4.2.2 Customer Information. The Supplier acknowledges that all customer-related information acquired during the provision of Services is considered Confidential Information of the Customer, and all rights, title, and interest in such Customer Information belong solely to the Customer. The Supplier shall use Customer Information only as necessary to perform Services in accordance with this Agreement and maintain Customer Information in strict confidence and in accordance with Section 4.2.1. Upon the Customer's request, the Supplier shall provide any or all Customer Information in the Supplier's possession.

4.3 Data Security; Privacy.

4.3.1 Data Security. The Supplier shall comply with the Customer's Security Policy, attached as Exhibit D, and any updates provided in writing by the Customer, provided such changes are commercially reasonable. The Supplier reserves the right to implement or modify security measures exceeding those in the Security Policy if deemed necessary for enhanced data protection. Such measures must meet or exceed industry standards and best practices, as well as the specific needs of the Supplier. The Supplier shall implement appropriate security measures to restrict access to Customer Data to only those personnel performing Services for the Customer under the applicable Service Order. The Supplier shall immediately notify the Customer of any security breach relating to the System and Services that may involve the Customer's Confidential Information or Customer Data, in accordance with Exhibit D.

4.3.2 Privacy. To the extent that Supplier is afforded access in any way to "Personal Data" as defined below, this Section 4.3.2 shall apply. The following definitions are relevant to this section: "Personal Data" shall derive its meaning from that which is set out in the EU General Data Protection Regulation 2016/679 (the "GDPR"). Personal Data shall also comprise any information that could be construed as "Personal Information" under the California Consumer Protection Act 2018 (the "CCPA"). "Sensitive Data" means as is set out in Article 9(1) of the GDPR. "Processing" (including its cognate, "Process") means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deletion, erasure, or destruction. "Data Security Breach" means: (A) the loss or misuse (by any means) of Personal Data; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Personal Data; or (C) any other act or omission that compromises the security, confidentiality, or integrity of Personal Data. "Technical and Organizational Security Measures" means security measures, consistent with the type of Personal Data being Processed and the services being provided by Supplier, to protect Personal Data, which measures shall implement best industry protections and include physical, electronic and procedural safeguards to protect the Personal Data supplied to Supplier against any Data Security Breach, and any security requirements, obligations, specifications or event reporting procedures set forth in any Service Order to this Agreement. As part of such security measures, Supplier shall provide a secure environment for all Personal Data and any hardware and software (including servers, network, and data components) to be provided or used by Supplier as part of its performance under this Agreement. Personal Data shall at all times remain the sole property of the Customer, and nothing in this Agreement will be interpreted or construed as granting Supplier any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right to Personal Data. Supplier shall Process Personal Data only on the instruction of the Customer and in accordance with this Agreement and applicable Data Protection Legislation and security laws, including but not limited to the GDPR and the CCPA. the Customer hereby instructs Supplier, and Supplier hereby agrees, to Process Personal Data as necessary to perform Supplier's obligations under this Agreement and for no other purpose. The Parties acknowledge that The Supplier will not store any Personal Data under this Agreement unless specified in a Service Order. It is understood and agreed that, if the Customer elects to store Personal Data in a System despite a Service Order not contemplating the same, Supplier shall not be responsible for the control, management, or protection of such Personal Data. the Customer acknowledges and agrees that it is solely responsible for any and all consequences resulting from its decision to store Personal Data in any such system. Supplier shall not create or maintain data which are derivative of Personal Data except for the purpose of performing its obligations under this Agreement and as authorized by the Customer. At any and all times during which Supplier is Processing Personal Data, Supplier shall:

a. Comply with all applicable Data Protection Legislation and security laws to which it is subject, including, but not limited to the GDPR and the CCPA, and not, by act or omission, place the Customer in violation of any applicable Data Protection Legislation or security law;

b. Have in place all appropriate and reasonable Technical and Organizational Security Measures to protect the security of Personal Data and prevent a Data Security Breach, including, without limitation, a breach resulting from or arising out of Supplier's internal use, Processing or other transmission of Personal Data, even where such use involves transmitting such to another person or entity acting on behalf of Supplier;

c. Safely secure or encrypt all Personal Data during storage or transmission;

d. Not use or maintain any Personal Data on a laptop or other portable device;

e. Notify the Customer promptly from the date of suspecting or obtaining actual knowledge of any Data Security Breach and, at Supplier's cost and expense, assist and cooperate with the Customer concerning any disclosures to affected Parties.

f. Not permit any officer, director, employee, agent, other representative, subsidiary, affiliate, or any other person or entity acting on behalf of Supplier to Process Personal Data unless such Processing is in compliance with this Agreement and is necessary in order to carry out Supplier's obligations under this Agreement;

g. Not disclose Personal Data to any third party (including, without limitation, any person or entity acting on behalf of Supplier) unless with respect to each such disclosure: (A) the disclosure is necessary in order to carry out Supplier's obligations under this Agreement; (B) Supplier has received the Customer's prior written consent, it being understood that such consent is hereby given for the sub-processors (if any)

h. Establish policies and procedures to provide all reasonable and prompt assistance to the Customer in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of any Personal Data Processed by Supplier or a supervisory authority.

Upon the Customer's request, Supplier shall provide evidence that it has established and maintains Technical and Organizational Security Measures governing the Processing of Personal Data appropriate to the Processing and the nature of the Personal Data to be protected. The Customer shall have the right to conduct unfettered onsite inspections and/or audits (upon reasonable advance notice to Supplier) of Supplier's information security protocols, and Supplier agrees to cooperate with the Customer regarding such inspections or audits. Supplier will promptly correct any deficiencies in the Technical and Organizational Security Measures identified by the Customer. Supplier shall return, delete, or destroy (at the Customer's election), or cause or arrange for the return, deletion, or destruction of, all data processed by the Customer within the Supplier environment, including, but not limited to the Customer Data and Personal Data subject to this Agreement, including, without limitation, to all originals and copies of such Personal Data in any medium and any materials derived from or incorporating such Personal Data, upon the expiration or earlier termination of this Agreement, or when there is no longer any legitimate business need (as determined by the Customer) to retain such Personal Data, the Customer Data or otherwise on the instruction of the Customer, but in no event later than thirty (30) days from the date of such expiration, earlier termination, expiration of the legitimate business need, or instruction. If applicable law prevents or precludes the return or destruction of any Customer Data or Personal Data, Supplier shall notify the Customer of such reason for not returning or destroying such data and shall not process such Personal Data or the Customer Data thereafter without the Customer's express prior written consent. Supplier's obligations under this Agreement to protect the security of Personal Data shall survive termination of this Agreement. The Supplier represents that its security measures comply with requirements specified in Exhibit D. In the event of updates to Exhibit D, Supplier will have a period of six months from the date of the change to review, evaluate, and implement necessary updates to ensure compliance with these best practices.

4.4 Audit.

The Customer may audit and verify The Supplier's compliance with this Agreement. Such audit will be conducted on prior written notice at the expense of the Customer and will be performed during Supplier's normal business hours. In addition, at the Customer's request, the Supplier will certify in writing to the Customer that it is in compliance with this Agreement in accordance with section 4.3.2 of this Agreement.

4.5 Material Breach.

Failure by Supplier to comply with the requirements of this section 4 shall constitute a material breach of this Agreement.

5. Representations and Warranties

Supplier represents and warrants that:

(a) the System and Services will conform to the criteria, requirements, applicable performance capabilities, characteristics, and other descriptions and standards for the System or Services set forth in this Agreement, and in any specifications and documentation specified or referenced in a Service Order (collectively "Specifications");

(b) it will perform the Services in a competent and workmanlike manner in accordance with the level of professional care customarily observed by highly skilled professionals rendering similar services, (though the Customer acknowledges that the Services are powered by Artificial Intelligence (AI) technologies which have inherent limitations and do not yet fully match the competencies of highly skilled professionals and can contain errors and biases);

(c) the System, Written Deliverables, Work Product and other materials provided by or on behalf of Supplier will not knowingly violate or infringe any third party's Intellectual Property rights;

(d) it has all rights necessary for (and is not subject to any restriction, penalty, agreement, commitment, law, rule, regulation or order which is violated by) its execution and delivery of this Agreement and performance of its obligations under this Agreement;

(f) the System, Written Deliverables, and Work Product do not contain any copy protection, automatic shut-down, lockout, "time bomb" or similar mechanisms that could interfere with the Customer's exercise of its business or its rights under this Agreement; and

(g) the System and Work Product to the best of its knowledge do not contain any viruses, "Trojan horses" or other harmful code. The Supplier cannot guarantee that the Services will be uninterrupted, error-free, do not contain any form of bias and do not inadvertently generate potentially harmful content. In accordance with applicable law, the Services, and Work Product are delivered to the Customer in their current state, fully operational and ready for use. Supplier is committed to providing a robust and effective solution. Supplier disclaims warranties of merchantability, optimal performance, or suitability for a specific purpose, but stands by the quality and integrity.

6. Limitations on Damages and Liability

Except for damages or liabilities arising under a Supplier's indemnification obligations pursuant to this agreement, or to the extent arising out of Supplier's willful misconduct or gross negligence or any breach of sections 5, Supplier's will not be liable (whether in contract, warranty, tort (including negligence) or otherwise) to the customer for damages for any indirect, incidental, or consequential damages arising out of or relating to this agreement, even if the Customer has been advised of the possibility of such damages. The Customer's liability arising from this agreement, whether in construct, tort or otherwise, will not exceed the greater of the aggregate amount of all fees and charges paid or payable by the customer under this agreement.

7. Indemnification

7.1 Indemnification. Supplier will defend, indemnify, and hold harmless the Customer and its Affiliates and the officers, directors, employees, successors, assigns, licensees, distributors, contractors, and agents of the Customer and its Affiliates (collectively, "Indemnified Parties") from all claims, damages, liabilities, assessments, losses, costs, and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses) arising out of or resulting from any claim, demand, suit, action or any other proceeding by a third party that arises out of or relates to:

(a) Supplier's actual or alleged breach of any of its warranties, representations and obligations in this Agreement, including Supplier's obligations with respect to the Customer Data and any Confidential Information of the Customer;

(b) any actual or alleged negligent act or omission, willful misconduct of either party;

(c) the Customer's use of the Services, System, Written Deliverables or Work Product; including any actual or alleged infringement, misappropriation or violation of any Intellectual Property or other right of any third party or breach of any third party's contractual terms or policies in connection with the Services, System, Written Deliverables or Work Product to the extent such infringement is not the result of the Customer's use of the Services in breach of this Agreement;

or (d) any actual or alleged personal or bodily injury (including, without limitation, illness or death) or damage to property caused by Supplier.

7.2 Procedure. Supplier will at all times keep the Indemnified Parties advised of the status of each claim and the defense of such claim. The Indemnified Parties will cooperate (at Supplier's cost with Supplier in the defense. Any Indemnified Party may participate in the defense at its own expense. If at any time any Indemnified Party reasonably determines that any claim might adversely affect any Indemnified Party, such Indemnified Party may take control of the defense of the claim at such Indemnified Party's expense (without limiting Supplier's indemnification obligations), and in such event such Indemnified Party and its counsel will proceed diligently and in good faith with such defense. Supplier will not consent to the entry of any judgment or enter into any settlement without the Indemnified Parties' prior written consent, which may not be unreasonably withheld. Supplier's duty to defend is independent of its duty to indemnify.

8. Ownership Rights

8.1 The Customer. The Customer owns and reserves all right, title and interest in and to the Customer Data and all Intellectual Property rights in or to any of the foregoing ("The Customer Intellectual Property"). Except as may expressly be set forth in this Agreement, no right, title, or interest to any of the Customer Intellectual Property is transferred or licensed to Supplier. Except as expressly provided in this Agreement, Supplier has no right to use or disclose any Customer Data.

9. Term and Termination

9.1 Term. The term of this Agreement (the "Term") begins on the Effective Date and, unless earlier terminated pursuant to this Agreement, continues for a period of one year. Upon expiration of such period, this Agreement will automatically renew on a month-to-month basis until the Customer gives at least sixty (60) days prior written notice of termination, provided, however, the terms of this Agreement will apply to any Service Order in effect as of the date of termination. The Customer may terminate this Agreement or any Service Order for any or no reason, by giving at least thirty (30) days prior written notice to the Supplier. Supplier may terminate this Agreement or any Service Order by giving at least sixty (60) days prior written notice to the Customer. Further, either Party may terminate this Agreement if the other Party materially breaches its obligations under this Agreement and fails to cure such breach within thirty (30) days of receipt of written notice from the other Party describing the breach in reasonable detail. Upon any termination of this Agreement, the Customer is only liable to pay for Services performed and liabilities incurred prior to expiration or termination. In connection with the termination or expiration of this Agreement for any reason, Supplier will provide reasonable assistance to the Customer in order to enable and facilitate an orderly transition of the Services to the Customer or to another vendor.

9.2 Data. Upon expiration or any termination of this Agreement or any Services provided hereunder, Supplier will provide the Customer all the Customer Data contained in the System or otherwise in the possession or control of Supplier in a format and media reasonably acceptable to the Customer and will destroy all such the Customer Data pursuant to Exhibit D.

9.3 Survival. Sections 4, 7, 8, 9, 10 and 11 (together with all other provisions hereof, including, without limitation, all Exhibits and other attachments hereto, that may be reasonably interpreted as surviving termination or expiration of this Agreement) will survive the termination or expiration of this Agreement.

10. Miscellaneous

10.1 Assignment. Supplier will not assign this Agreement, in whole or in part, without the Customer's prior written consent. Any attempt to assign in violation of this Section is void in each instance. the Customer may assign this Agreement (or any of its rights and obligations under this Agreement or any Service Order): (a) to any of its Affiliates; or (b) in connection with any merger, consolidation, reorganization, sale of all or substantially all of its assets or any similar transaction. All the terms and conditions of this Agreement will be binding upon, will inure to the benefit of, and will be enforceable by the Parties and their respective successors and permitted assigns.

10.2 Entire Agreement. This Agreement, together with all associated exhibits, schedules, and Service Orders, all of which are incorporated by this reference, constitute the complete and final agreement of the Parties pertaining to the Services and supersede the Parties' prior agreements, understandings and discussions relating to the Services. No modification of this Agreement is binding unless it is in writing and signed by the Customer and Supplier. This Agreement, any Service Orders and amendments may be executed electronically and may be signed in counterparts (which may be scanned copies), which together will constitute one agreement. The Parties may use standard business forms or other communications, but use of such forms is for convenience only and does not alter the provisions of this Agreement.

10.3 Governing Law. This Agreement will be interpreted, construed and enforced in all respects in accordance with the laws of Spain without reference to its choice of law rules. Except as set forth below, competent courts seated in Barcelona shall have sole and exclusive jurisdiction for all purposes in connection with any action or proceeding that arises from, or relates to, this Agreement, and you hereby irrevocably waive any objection to such exclusive jurisdiction; provided however, that LIGHTENUP EUROPE S.L. may seek to enforce any judgment in its favor in any court of competent jurisdiction. Notwithstanding the foregoing, LIGHTENUP EUROPE S.L. may seek injunctive or other equitable relief in any court of competent jurisdiction to protect its proprietary and other rights.

10.4 Independent Contractor. Supplier is an independent contractor for the Customer in connection with the Services it provides under this Agreement, and nothing in this Agreement is intended to create or shall be construed as creating an employer-employee relationship or a partnership, agency, joint venture, or franchise. Upon request, Supplier shall provide the Customer with satisfactory proof of independent contractor status (including a valid business license in the State/Country in which Supplier is incorporated). Under no circumstance will one Party's employees be construed to be employees of the other Party, nor will one Party's employees be entitled to participate in the profit sharing, pension or other plans established for the benefit of the other Party's employees. Supplier will have no authority to enter into any agreement on the Customer's behalf or in the Customer's name.

10.5 Notices. All notices, authorizations, and requests in connection with this Agreement will be deemed given (a) one (1) day after they are sent by air express courier, charges prepaid, or (b) on the day of transmittal if sent by email (but only in those instances where the recipient confirms receipt), in each case to the address set forth above or to such other address as the Party to receive the notice or request so designates by written notice to the other. E-mail notices to Supplier must be sent to legal@lightenup.ai and e-mail notices to the Customer must be sent to <customer email>.

10.6 Severability. This Agreement will be enforced to the fullest extent permitted by applicable law. If any provision of this Agreement is held to be invalid or unenforceable to any extent, then the remainder of this Agreement will have full force and effect and such provision will be interpreted, construed or reformed to the extent reasonably required to render the same valid, enforceable and consistent with the original intent underlying such provision.

10.7 Waivers and Remedies. No waiver of any term, condition or obligation of this Agreement will be valid unless made in writing and signed by the Party to which such performance is due. No failure or delay by any Party at any time to enforce one or more of the terms, conditions or obligations of this Agreement will (a) constitute waiver of such term, condition or obligation, (b) preclude such Party from requiring performance by the other Party at any later time, or (c) be deemed to be a waiver of any other subsequent term, condition or obligation, whether of like or different nature. The remedies specified in this Agreement are in addition to any other remedies that may be available at law or in equity.

10.8 Class Action Waiver: To the maximum extent permitted by law, the Customer and Supplier agree that all claims against each other can only be brought in an individual capacity and not as a plaintiff or class member in any purported class, consolidated, or other representative proceeding. We agree that arbitrators may not conduct any class, consolidated, or representative proceeding and are limited to providing relief warranted by an individual party's claim.

10.9 Restriction of Services: Supplier reserves the right, at its sole discretion, to restrict or block the provision of Services under this Agreement in instances where Supplier has reason to suspect fraudulent or abusive behavior that impacts or is likely to impact delivery of the Services or the Customer's receipt thereof. This includes, but is not limited to, activities that jeopardize the integrity and security of Supplier's System, the Customer Data, or that which might otherwise violate applicable laws or this Agreement. In such cases, Supplier will take appropriate action as necessary to protect its and the Customer's interests and will promptly notify the Customer of such measures, subject to applicable laws and regulations.

10.10 Force Majeure. Neither Party shall be in breach of this Agreement or otherwise liable for any failure or delay in the performance of its obligations if such delay or failure result from events, circumstances or causes beyond its reasonable control. The time for performance of such obligations shall be extended accordingly. If the period of delay or non-performance continues for four (4) weeks, the Party not affected may terminate this Agreement by giving fifteen (15) days' written notice to the affected Party. If the Customer is the terminating Party, Supplier shall promptly reimburse to the Customer all prepaid sums for the unexpired Term.

10.11 Language. All communications and notices made or given pursuant to this Agreement must be in the English language. If either Party provides a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

10.12 Dispute Resolution. If a dispute arises under this Agreement (a "Dispute"), including without limitation any Disputes arising out of any amount due to a Party hereto, then prior to bringing any suit, action or proceeding in connection with such Dispute, a Party must first give written notice of the Dispute to the other Party describing the Dispute and requesting it be resolved pursuant to this dispute resolution process (the "Dispute Notice"). If the Parties are unable to resolve the Dispute within thirty (30) days of delivery of the Dispute Notice, then each Party shall promptly (but no later than thirty (30) business days thereafter) (a) appoint a designated representative who has sufficient authority to settle the Dispute and who is at a higher management level than the person with direct responsibility for the administration of this Agreement (the "Designated Representative"), and (b) notify the other Party in writing of the name and contact information of such Designated Representative. The designated representatives shall then meet as often as they deem necessary in their reasonable judgment in order to discuss the Dispute and negotiate in good faith to resolve the Dispute. The Designated Representatives shall mutually determine the format for such discussions and negotiations, provided that all reasonable requests for relevant information relating the Dispute made by one Party to the other Party shall be honored. If the Parties are unable to resolve the Dispute within sixty (60) days after the appointment of both Designated Representatives, then either Party may proceed with any other available remedy.

10.13 No Exclusivity; No Minimums. Unless otherwise specifically provided in the Schedule, the Parties hereto agree that nothing contained in this Agreement will be construed as creating an exclusive relationship between the Parties, and nothing in this Agreement will prevent either Supplier or the Customer from entering into the same or similar relationship with others. Additionally, nothing herein will be construed as creating a minimum commitment for business on the part of the Customer to Supplier.

11. Definitions

In addition to the terms in initial capitalized letters defined elsewhere in this Agreement, the following terms in initial capitalized letters have the respective meanings set forth below.

"Account" means the unique user profiles, credentials, and/or access points provided by Supplier to the Customer, to provide access to the Services.

“Affiliate” means any entity that directly or indirectly controls, is controlled by or is under common control with the Customer.

“The Customer Data” means all Data (including, without limitation, End-User Data) (a) collected, received, stored or maintained by the System or Supplier from the Customer in connection with its use of the System or Supplier’s performance of its obligations under this Agreement, (b) provided by the Customer to Supplier, or (c) derived from (a) or (b).

“Data” means any data, records, files, content or information, in any form or format, including interim, processed, compiled, summarized, or derivative versions of such data, content or information.

"End User" means an individual who, as a customer of the Customer or an Affiliate, receives communications, messages, or other outputs generated by the System or Services. These End Users do not directly access or manipulate the System or Services but are the recipients of its functionality as intended and operated by the Customer.

“End-User Data” means any Data related to users of the Customer’s or its Affiliates’ websites or services (including End Users), whether personally identifiable or not, and regardless of type, amount or nature of information, including, without limitation, any information regarding any (a) natural person or other end-user; (b) any device (e.g., a computer, mobile or handheld telephone or tablet, or browser) used by a natural person or end -user to access or visit any web site or online service; and (c) any Data obtained through a pixel, cookie or other Data collecting mechanism.

"Feedback" means any comments, observations, opinions, or constructive criticism, provided by the Customer to Supplier, regarding the Supplier's services, products, or operations, based on the Customer's use and experience.

“Hosted Services” means the services provided and to be provided by Supplier to the Customer under this Agreement through the System, as is further described in a Service Order.

“Implementation Services” has the meaning set forth in Section 1.3.

“Intellectual Property” means any patent, copyright, trademark, or trade secret right and any other intellectual property or proprietary right in any jurisdiction, including any and all applications, registrations and rights of registration, reissues, divisions, continuations, continuations-in-part, substitutes, renewals, and extensions with respect thereto, any causes of action related to any violation, infringement or misappropriation thereof, and any income, royalties, damages and payments due or payable with respect thereto.

“Pre-existing Work” means: (a) any inventions or developments made by Supplier prior to the Effective Date (including the System); or (b) any improvements Supplier may make to its own proprietary software or any of its internal processes as a result of any Service Order, provided that such improvements do not infringe the Customer’s Intellectual Property rights.

“Professional Services” means any consulting or other services that are described in a Service Order that are not Hosted Services or Implementation Services.

“Services” means any services provided and to be provided by Supplier under this Agreement, including the Hosted Services, Professional Services and Implementation Services, and any associated deliverables or other results thereof.

"Service Interaction" means any request, transaction, action, or communication initiated between the Customer and Supplier through any agreed-upon medium, designed to facilitate the execution, delivery, or utilization of a Service. This includes, but is not limited to, API calls, data transmissions, user queries, and any other methods by which the Customer seeks to engage or utilize the Service provided. Service Interactions can be deemed successful or unsuccessful based on their ability to execute the intended function or deliver the specified Service as outlined in the corresponding Service Order.

“Service Order” means an order for Services executed by the Parties, the agreed to form of which is attached to this Agreement as Exhibit A.

"Suggestion" means any proposal, idea, recommendation, or possible course of action, provided by the Customer to Supplier pursuant to this Agreement, intended to improve, modify, or otherwise affect Supplier's services, products, or operations.

“System” means the software and other technology of the Supplier that the Customer may be required or have the option to use in order to access, use and receive Services, and any associated documentation made available to the Customer hereunder.

“Work Product” means any deliverables that Supplier must deliver to the Customer as part of any Professional Services pursuant to a Service Order, including but not limited to concepts, works, inventions, information, drawings, designs, programs, or software (whether developed by Supplier or any of its personnel, either alone or with others, and whether completed or in-progress), except that Work Product does not include Pre-Existing Work.

IN WITNESS WHEREOF, the Parties have executed this Agreement by their authorized representatives as of the Effective Date.

Exhibit A

FORM SERVICE ORDER

Service Order Form No. [INSERT NUMBER]
Supplier Name:
Customer:
Data Submitted:
Version:

This Service Order is entered into as of [INSERT DATE] (the "Service Order Effective Date") and is made a part of the Hyperflow AI Services Agreement between <Customer>("Customer") and LIGHTENUP EUROPE, S.L. ("Supplier"), with an effective date of <MSA effective date> (the "Agreement"). All capitalized terms not defined in this Service Order have the respective meanings set forth in the Agreement.

1. Name of Services or System

[LIST ANY SERVICE OR SYSTEM AND THEIR CATEGORIES]

2. Services categories and specifications

2.1. Hosted Services: Yes/No

[IF YES, PLEASE INSERT DETAILED DESCRIPTION OF HOSTED SERVICES TO BE PROVIDED]

2.2. Implementation Services: Yes/No

[IF YES, PLEASE INSERT DETAILED DESCRIPTION OF IMPLEMENTATION SERVICES TO BE PROVIDED]

2.3. Work Product: Yes/No

[IF YES, PLEASE INSERT DETAILED DESCRIPTION OF WORK PRODUCT TO BE PROVIDED]

2.4. Professional Services: Yes/No

[IF YES, PLEASE INSERT DETAILED DESCRIPTION OF PROFESSIONAL SERVICES TO BE PROVIDED]

3. Definitions of Service

[LIST ANY SERVICE OR SYSTEM TO BE PROVIDED]

4. Term

5. Delivery service order / Milestones

5.1. Milestones

5.2. Acceptance procedure and criteria

6. Services fees

6.1. Services fees

The Customer will pay Supplier a monthly fee of $[INSERT AMOUNT] for the Hosted Services ("Hosted Service Fees"), payable by the Customer pursuant to the terms of Section 2 of the Agreement. Supplier will invoice the Customer for the fees for Hosted Services monthly in arrears beginning upon the Customer's acceptance of the Implementation Services (if any).

[IF IMPLEMENTATION SERVICES OR PROFESSIONAL SERVICES ARE PROVIDED, THEN INCLUDE THE FOLLOWING] the Customer will pay Supplier $[INSERT AMOUNT], [optional: with an aggregate total not to exceed $_____, including any pre-approved costs and taxes,] for the [Professional/Implementation] Services performed by Supplier in accordance with the Agreement ("Professional/Implementation Service Fees"). The Customer will pay Supplier THE Professional/Implementation Service Fees after completion of the Professional/Implementation Services [or in accordance with the delivery of deliverables as set forth above] and acceptance by the Customer.

6.2. Usage cap

This total number of interactions with AI Chat Services, AI Services and AI Custom Services per month is _____ ("Usage Cap").

6.3. Payment terms

All payments under this Service Order are subject to the Customer's receipt of Supplier's invoice. The invoice will be in a form and content reasonably acceptable to the Customer and will contain sufficient information to allow the Customer to determine the accuracy of the amounts billed. Payment terms are net sixty (60) days of receipt of invoice and acceptance of Services by the Customer, pursuant to the terms of Section 2 of the Agreement.

This Service Order is entered into as of the Service Order Effective Date.

The Customer:

[FILL IN APPROPRIATE THE CUSTOMER

ENTITY]

By:

Printed Name:

Title:

Date Signed:_____

Supplier:

[INSERT SUPPLIER ENTITY NAME]

By:

Printed Name:

Title:

Date Signed:_____

Exhibit B

MAINTENANCE AND SUPPORT

Supplier will maintain and support the System to ensure solid and reliable connectivity and access by the Customer, its Affiliates and their users and that the System performs and operates with in accordance with the Specifications and as set forth in this Exhibit and the other terms and conditions of this Agreement. Supplier will promptly repair or replace, without any additional charge, the System or any portion thereof, that have any bugs, defects or errors (collectively, "Errors"). The Supplier will provide the support services on a 24x7 basis, 365 days per year.

Updates and Upgrades

Supplier will update the System and make available to the Customer any and all patches, enhancements, updates, upgrades and new versions of the System or Supplier Furnished Materials that Supplier makes generally commercially available ("Updates"). Any such Updates will be deemed part of the System as that term is used herein and will be covered by the maintenance and support services set forth in this Exhibit. Supplier represents and warrants that no Update (i) will impair the operation or disable or inhibit any functions or features of the System or cause a loss of functionality as provided in the Specifications or cause performance of the System to be degraded; or (ii) adversely affect form, fit, function, reliability, safety or serviceability of the System or their compliance with all of the requirements of this Agreement.

Availability and Contacts

Supplier will make technical support available to the Customer by e-mail and a shared Slack channel twenty-four (24) hours per day, seven (7) days per week. Supplier's support personnel will provide the Customer with remote assistance for help in using and operating the System and to accept reports of Errors in the System. Supplier will ensure that each of its personnel performing any maintenance and support services are experienced, knowledgeable and qualified in the use, maintenance and support of the System. Contact information for technical support is as follows:

E-mail: support@lightenup.ai

Supplier may change any of the foregoing contact information from time to time by delivery of not less than thirty (30) days prior written notice to the Customer, so long as at least one number or address is at all times available for each means of contact.

Error Correction: In the event that the Customer reports to Supplier any Error in the System, Supplier will respond to such reports as follows:

"Severity Level 1" is an emergency condition which directly impacts the Customer's mission-critical functionalities. These are functionalities essential for the core operations of the Customer. This severity 1 issue makes the use or ongoing operation of one or more of these critical functionalities impossible or significantly impaired. The condition requires an immediate solution that is not already available to the Customer.

"Severity Level 2" is, other than any Severity Level 1 Problem, any substantial issue or condition which makes the use or continued use of any one or more functions of the System impossible or significantly impaired and which the Customer cannot reasonably circumvent or avoid on a temporary basis without the expenditure of significant time or effort.

"Severity Level 3" is, other than any Severity Level 1 Problem or Severity Level 2 Problem, any limited issue or condition which is not critical in that no loss of the Customer Data occurs and which the Customer can reasonably circumvent or avoid on a temporary basis without the expenditure of significant time or effort.

"Severity Level 4" is, other than any Severity Level 1 Problem, Severity Level 2 Problem or Severity Level 3 Problem, a minor problem condition or Documentation error which the Customer can easily circumvent or avoid.

Response Times:

Supplier will respond to an Error, depending on the Severity Level, within the time frames set forth in the table below, starting from the time the Customer notifies Supplier of the Error.

Severity Level Response Time:

Severity	Response Time
Level 1	30 mins
Level 2	1 hour
Level 3	2 hours
Level 4	6 hours

The Supplier will provide maintenance and support services at no additional charge.

Exhibit C

PERFORMANCE STANDARDS

1. Service Level Standards. Supplier will at all times during the term of this Agreement maintain the following service levels for the Services (collectively, the "Service Levels"):

1.1 System Availability Service Level. Supplier will provide 97% System Availability over one-month periods, excluding any System Maintenance or Force Majeure Events (as defined below) that result in the System not being available to the Customer, as measured and monitored from Supplier's facilities.

System Availability will be calculated on a monthly basis using the following formula:

[(Actual Availability divided by Total Scheduled Availability) multiplied by 100%].

The following definitions will apply with respect to the calculation of Service Availability:

(a) "Actual Availability" means Total Scheduled Availability minus Downtime, in minutes. (b) "Downtime" means the time (in minutes) that users of the System are not able to (a) access the System, (b) perform ordinary functions to use or receive Services in accordance with Specifications, or (c) utilize the System and Services for normal business operations due to failure malfunction or delay. Downtime does not include any unavailability of the System due to System Maintenance or a failure or defect arising out of a Force Majeure Event.

(c) "Force Majeure Event" means any failure or delay caused by or the result of causes beyond the reasonable control of a Party and could not have been avoided or corrected through the exercise of reasonable diligence, including, but not limited to fire, flood, hurricane or other natural catastrophe, terrorist actions, Laws, or any civil or military authority, national emergency, insurrection, riot or war, or other similar occurrence.

(d) “System Maintenance” means time (in minutes) that the System is not accessible to the Customer due to maintenance of the System, including for maintenance and upgrading of the software and hardware used by Supplier to provide the Services. System Maintenance includes scheduled maintenance and unscheduled, emergency maintenance. Supplier will provide the Customer with at least ten (10) business days’ prior written notice of any scheduled maintenance or sixty minutes’ advance written notice for unscheduled, emergency maintenance. Supplier will provide such notices to the Customer by email to an address provided by the Customer or by displaying notifications prominently within the user interface. These notifications will be strategically placed in sections of the interface that are clearly visible to users when they access their accounts on the system. System Maintenance in any given month will not exceed sixty minutes per month, and will only be performed on Friday or Saturday between the hours of 1:00 a.m. and 3:00 a.m. (CET). Any time during which the System is unavailable to the Customer due to maintenance or other activity by Supplier for which Supplier fails to give notice, which exceeds the permitted time allotment, or which occurs outside of the foregoing permitted hours will be included in the calculation of Downtime.

(e) “Total Scheduled Availability” means seven (7) days per week, twenty-four (24) hours per day, excluding System Maintenance, in minutes.

2. Reporting. During the term of this Agreement, Supplier will, upon the Customer’s request (which can be made by email), provide monthly reports to the Customer that include Supplier’s performance with respect to the Service Levels and such other metrics as reasonably requested by the Customer from time-to-time.

3. SLA Credits. If Supplier fails to meet any of the Service Levels, Supplier will pay the Customer penalties calculated as follows (the “SLA Credits”):

3.1 SLA Credits for Service Availability Service Level Failure. If the System Availability during any given month falls below 98%, Supplier will provide the Customer with an SLA Credit equal to the percentage of the total monthly hosting fee applicable to the month in which the Service Level failure occurred corresponding to the System Availability Level set forth below:

- 97.1-100% - No credit will be provided
- 96.1-97% - 10% of total monthly fee applicable to month in which failure occurred
- 95-96.1% - 25% of total monthly fee applicable to month in which failure occurred
- < 95% - 30% of total monthly fee applicable to month in which failure occurred

3.2 SLA Credit Procedures. Supplier will credit all SLA Credits accrued to the Customer in the month in which the SLA Credits accrue, provided that if no further invoices will be submitted to the Customer hereunder, Supplier will pay such SLA Credits to the Customer within thirty (30) days of the end of the month in which such SLA Credits accrue.

3.3 Chronic SLA Failure. In addition to the SLA Credits set forth in Section 4.1 above, if Supplier fails to meet any Service Level in any two (2) months in a rolling six month period during the term of this Agreement, the Customer will have the right in its sole discretion to terminate the Services immediately upon written notice to Supplier.

Exhibit D

INFORMATION SECURITY EXHIBIT

Security and privacy sit at the core of product development at lightenUp (hereinafter, "Supplier"). This Information Security Exhibit (the"Exhibit") describes the organizational policies, strategies and controls in effect at lightenUp that are aimed towards maintaining confidentiality, integrity, and availability of Customer Data used with lightenUp products or services (hereinafter, the "Software"). Unless defined herein, terms used with capital letters will have the meaning given to them in the applicable Agreement.

DEFINITIONS:

"Agreement" means the agreement validly executed between lightenUp and the Customer with respect to access to, and use of, paid Software and/or Services, and incorporates this Exhibit.

"Cloud Software" means the Solution as a service provided to the Customer.

"Customer" means the entity using paid Software and/or Services under a Service Contract.

"Customer Data" means any data, information, and proprietary Customer content created prior to or independently from any Customer interaction with the Software and imported into the Software, or accessed by lightenUp in connection with, or for the purpose of, provision of any Services. Customer Data may contain Personal Data.

"Documentation" means the official public user documentation for Software as made available by lightenUp.

“Personal Data” means (i) information related to an identified or identifiable natural person as defined by, as applicable, Regulation (EU) 2016/679 (“GDPR”), the California Consumer Privacy Act (“CCPA”), and other applicable privacy laws.

“Services” means professional services specified in an Order, excluding Support.

“Solution” means software products developed by or for lightenUp and/or its Affiliates and licensed to Customer as specified in accepted orders, which may be provided, as available as Cloud Software, and excludes Third-Party Services.

“Support” means maintenance and service, applicable to the Software during the License Term or as mutually agreed with the Customer.

“Third-Party Services or sub-processors” means the cloud applications, cloud service endpoints, data services, software, application programming interfaces, AI services and content of third parties which may be accessed using the Solution or Services.

“lightenUp Internal Policies” means the collection of policies maintained available by lightenUp with respect to confidentiality, information security, and intellectual property protection.

SCOPE

This Exhibit highlights security measures maintained by lightenUp with respect to its internal infrastructure and its Solution, that could have an impact on the confidentiality, integrity, and availability of Customer Data. This Exhibit does not cover any standards maintained by providers of Third-Party Services or sub-processors.

PRODUCT SECURITY

1. Product Development Practices

LightenUp follows security best practices to ensure a secure software development lifecycle ("SDLC") for developing products. The secure SDLC process includes a DevSecOps framework that performs security scans at every release. The DevSecOps framework includes but is not limited to code reviews, threat modeling during service design and security assessments such as static and dynamic code analysis and manual penetration testing.

LightenUp is committed to evaluating changes to systems and applications, which includes applicable security controls. Before any changes to systems or applications are implemented, they must satisfy predetermined acceptance standards and also require stakeholder approval prior to change implementation as applicable..

Furthermore, lightenUp limits access to the software's source code and developers participate in training sessions on secure system development on a regular basis.

2. Cryptographic Controls

Encryption is a crucial element of lightenUp's security approach, designed to safeguard information from unauthorized access.

Customer Data is encrypted both in transit and at rest using standards that comply with applicable laws and regulations. For instance, data is encrypted using AES-256 while stored in databases, and TLS 1.2 or higher is used for data transmission over networks.

3. Network Security and Segregation

A WAF solution is implemented to provide protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.

Development and production environments per tenant are fully physically segregated across multiple zones to ensure security, compliance with Data privacy policies and high availability.

LightenUp backend services and databases are isolated in private networks protected by cloud firewalls that allow traffic only from authorized protocols, ports, sources and identities.

4. Access Controls

Programmatic access is allowed through robust authentication and authorization protocols. This includes the use of OAuth2 and JWT tokens for user sessions, managed by AWS Cognito.

Multi-Factor Authentication (MFA) is enforced for all access to lightenUp systems, requiring users to provide a password and a one-time code sent to their mobile device before accessing their accounts or making changes to security settings.

5. Access to Customer Data

lightenUp core product, Hyperflow, service offering includes a CRUD APIs that allows Customer admin users to ingest, read, update and delete any Customer data stored and used by lightenUp's Solutions.

6. Customer Data Back-ups

lightenUp performs regular backups of Customer Data, which are stored in multiple locations to ensure resiliency.

7. Customer Data Retention

As a rule, Customer Data is kept for the duration of the Agreement.

Following termination of the Agreement and upon express written instructions from the Customer, lightenUp will ensure that the Customer Data will be, as requested by the Customer in the timeframe specified by the applicable law, deleted, or returned to the Customer either manually or, if technically available, via direct export from the relevant Cloud Software.

8. Logs Information

The Software includes logging capabilities that are always active. These logs capture informational events, errors, warnings, and audit trails for actions performed within the Software.

AWS services, such as CloudWatch, are utilized for secure log storage and management. For example, all login attempts, file uploads, and administrative changes to system configurations are logged.

9. Personal Data Protection

At LightenUp, we only process data that the Customer provides through our platform or APIs. Our platform is not open to the public; only contracted customers have access.

We do not collect or process data from any other sources. Moreover, we do not generate revenue from selling ads or user data. The Customer data is solely used to provide our services to the Customer.

At LightenUp, we prioritize the Customer privacy by storing in the user cookies only the minimal amount of data necessary to help the Customer use the platform effectively. We will never collect or use any data for selling to other companies or third parties for any kind of tracking purposes.

The protection of Personal Data is a shared responsibility among the Customer, LightenUp, and the Cloud Services (AWS):

LightenUp Responsibility: LightenUp is responsible for protecting the infrastructure, services, configuration and management of the entire platform. This includes configuring the environment, managing Customer data (including encryption options), classifying assets, and implementing authentication and authorization mechanisms to apply appropriate permissions. LightenUp ensures that the platform is securely implemented, configured and maintained to meet the highest standards of data protection. lightenUp makes available a process for data subject access requests, as required by the GDPR. LightenUp also provides a process for handling data subject access requests, as required by the GDPR.

Customer Responsibility: The Customer is responsible for ensuring that all data ingested into the platform complies with applicable legal and regulatory requirements. This includes ensuring that the data provided to LightenUp for processing is lawful and does not violate any legal standards. The Customer must ensure that they have obtained all necessary consents and legal authorizations for the data they submit to the platform, thereby allowing LightenUp to process it without any legal issues arising.

10. Vulnerabilities Management

Vulnerabilities discovered in the Software are classified according to the industry-standard Common Vulnerability Scoring System ("CVSS") methodology (i.e., critical, high, medium, and low). Remediation of identified vulnerabilities is carried out promptly within timeframes set internally.

Regular testing is conducted to detect vulnerabilities in the Software and its associated ecosystem to safeguard Customers' usage of the Software from harmful activities.

lightenUp conducts penetration tests for Cloud Software systems and applications that handle Customer Data, including after substantial system and application modifications. lightenUp will establish a patch and vulnerability management process to identify, document, and rectify application and system vulnerabilities that is sanctioned by the application or system owner and is proportionate to the level of risk.

INTERNAL SECURITY PRACTICES

1. Access Controls

lightenUp employees are provided logical access to corporate resources for which they have received explicit authorization, in line with established access control policies and processes. These access privileges are granted as necessary for staff members to perform their responsibilities, adjusted when there is a change in role, and revoked upon termination of employment.

Owners of applications are required to assess user access rights for suitability on a regular basis and are obligated to immediately withdraw any inappropriate or unauthorized access upon discovery.

lightenUp employs a strong password policy, along with MFA sign-on on all enterprise applications and systems. For Customer end user authentication, lightenUp shall support authentication and authorization to access the resources. By policy, users are obligated to keep their passwords confidential and to change them at regular intervals.

The logical access of users to business applications is controlled. lightenUp has activated logging for sign-in activities on systems and produces alerts for abnormal sign-in behavior.

Access to business systems and applications shall be based on the principles of least privilege and segregation of responsibilities.

In relation to privileged user accounts, lightenUp will (a) limit access to members with explicit business requirements; (b) allocate accounts only for the time required to accomplish the necessary task, c) record and periodically examine system logs, and (d) facilitate access using multi-factor authentication.

2. Risk Management

lightenUp regularly assesses and mitigates risks related to its operations and the security of its systems.

Periodic risk assessments are conducted to identify new threats, and additional controls are implemented to address high-risk areas.

3. Asset Management

lightenUp's information assets are safeguarded throughout the information lifecycle, including entry into lightenUp systems, secure data transmission, and suitable data access, storage, retention, and disposal. lightenUp's information assets are properly classified in terms of value, legal and contractual requirements to guide employees in handling them appropriately.

lightenUp requires its employees and contractors to comply with a set of security measures when handling lightenUp devices and information. Each lightenUp asset holding confidential information has an identified asset owner and is kept in an inventory that covers the entire lifecycle from purchase to disposal.

lightenUp shall implement and document system hardening procedures and baseline configurations and shall not include unsupported software or hardware.

3.5. Disposal and Destruction of Data and IT Equipment. lightenUp has controls in place to mitigate the risk of improper and unsecure disposal and destruction of data, technology equipment and components owned by lightenUp, including over writing, or physically destroying removable media, erasing, or destroying mobile devices and securely erasing storage space allocated by cloud services, according to the cloud provider's methodology.

lightenUp maintains policies in place restricting the storage of Customer Data locally, on the employees' devices or on removable media.

4. Mobile Devices and Teleworking

Since lightenUp does not provide physical office space or company-issued devices, employees use personal devices for work purposes. lightenUp enforces security policies that require employees to secure their devices with strong passwords, encryption, and up-to-date antivirus software.

lightenUp implements various security measures on employee devices, including enforcing a multi-factor authentication access control mechanism to grant full access to Customer Data.

5. Human Resources Security

lightenUp may conduct background checks prior to employment, always in compliance with relevant laws.

lightenUp guarantees that employees consent to confidentiality and information security terms and conditions commensurate with their access levels to organizational assets, extending beyond their employment tenure.

Clear communication of information security responsibilities is provided to lightenUp employees, accompanied by an understanding that policy and procedure breaches may result in disciplinary measures.

6. Vendor Risk Management

lightenUp maintains a vendor risk management program through which it assesses and manages the risks assumed by the nature of relationships with vendors and contractors that receive, store, process, or host lightenUp data or have access to lightenUp systems.

lightenUp checks the security measures of its critical vendors and has a policy to enter into data protection agreements seeking to ensure that at least the same level of confidentiality and data security is implemented by its subcontractors as the ones applicable to lightenUp.

lightenUp strives to maintain the right to perform audits to monitor the compliance of its subcontractors with the agreed technical and organizational measures regarding data confidentiality and security.

INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

lightenUp is dedicated to fulfilling contractual and legal obligations regarding the safeguarding of Customer Data. It has established protocols to promptly address security and operational incidents, ensuring minimal risks and uninterrupted availability of information systems.

To ensure swift and efficient incident response, lightenUp's incident management teams undertake necessary measures to contain threats, eliminate the source of incidents, and restore affected systems, information, and data.

Incident responders meticulously analyze incident root causes, integrate lessons learned into the incident management system, and propose continuous enhancements to system and data integrity.

lightenUp adopts a decentralized office model, allowing employees and contractors to operate independently of specific locations. Data processing environments are designed with redundancy to meet availability demands, incorporating failovers within availability zones. Continuity of service and data availability are upheld through reputable cloud service providers.

As part of lightenUp's commitment to incident management, lightenUp will establish and uphold a formally documented incident management policy.

lightenUp conducts business continuity risk assessments to identify relevant risks, threats, likelihood of service outages or security breaches, and the potential impacts thereof. Following the risk assessment, LightenUp documents, implements, regularly tests, and reviews business continuity plans.

AWARENESS AND TRAINING

lightenUp conducts an internal training program aimed at educating employees on lightenUp's information security and compliance policies. This program ensures that employees understand the acceptable use of lightenUp resources, thereby reducing the risk of unauthorized access to company equipment and improper use or modification of information assets.

This training is updated to incorporate changes in organizational policies and procedures. It addresses employees' specific job roles, outlines disciplinary measures in the event of suspected or actual data breaches caused by personnel, and includes specialized training on handling personal data in compliance with relevant data protection laws.

POLICY MONITORING, TESTING AND REVIEWING

lightenUp regularly reviews and updates its security policies to ensure they align with industry standards, legal requirements, and business practices.

CUSTOMER ASSESSMENT

lightenUp is committed to promptly reviewing and completing any justified security questionnaires from customers. Upon written request, LightenUp will provide relevant documentation, reports, and evidence for customer review.

CHANGES TO THIS INFORMATION SECURITY EXHIBIT

We retain the right to modify this policy to align with new regulations, legal precedents, and evolving industrial or commercial practices. If any changes are made to our Information Security Exhibit, they will be published on our website https://www.lightenup.ai/.

Exhibit E:

TERMS OF SERVICE

This Terms of Service agreement (the "Agreement") is made between LIGHTENUP EUROPE, S.L. (the "Company"), and you, the customer (the "Customer"), and governs your access and use of the Company's software-as-a-service (Saas) application programming interface (API) offering (the "Service"). By accessing or using the Service, you agree to be bound by this Agreement. If you do not agree to this Agreement, you may not access or use the Service.

1. Service description

The Service is a SaaS API offering that allows the Customer to access and use various internal artificial intelligence (AI) services as well as third party AI providers, such as OpenAI, Azure, and Amazon Bedrock (the “AI Providers”). The Service acts as an intermediary between the Customer and the AI Providers, and does not create, own, or control the AI services or the results generated by the AI services. The Service merely facilitates the communication and integration between the Customer and the AI Providers, and provides the Customer with a unified and simplified interface to access and use the AI services.

2. License grant

The Company grants the Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to access and use the Service, solely for the Customer’s internal business purposes and in accordance with this Agreement and the Company’s documentation and policies. The Customer may not use the Service for any unlawful, fraudulent, or malicious purposes, or in any way that violates the rights or interests of the Company, the AI Providers, or any third parties. The Customer may not copy, modify, reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code or the underlying technology of the Service, or create any derivative works based on the Service. The Customer may not rent, lease, sell, resell, distribute, or sublicense the Service, or offer the Service as part of a service bureau or outsourcing service, or otherwise make the Service available to any third parties. The Customer may not interfere with or disrupt the operation, security, or performance of the Service, or attempt to gain unauthorized access to the Service or any related systems or networks. The Customer may not use any automated means, such as bots, scripts, or crawlers, to access or use the Service, or use the Service in a manner that exceeds the reasonable request volume or imposes an unreasonable burden on the Service or the AI Providers. The Customer may not remove, alter, or obscure any proprietary notices or labels on the Service or any results generated by the Service. All rights not expressly granted to the Customer are reserved by the Company and its licensors.

3. Customer data

The Customer is solely responsible for the data, content, and information that the Customer submits, uploads, or transmits to the Service or the AI Providers, or that the Service or the AI Providers collect, process, or store on behalf of the Customer (the "Customer Data"). The Customer represents and warrants that the Customer owns or has the necessary rights and permissions to use and share the Customer Data, and that the Customer Data does not infringe or violate the rights or interests of the Company, the AI Providers, or any third parties, or any applicable laws or regulations. The Customer grants the Company and the AI Providers a non-exclusive, royalty-free, worldwide license to access, use, copy, modify, store, transmit, and display the Customer Data, solely for the purpose of providing the Service to the Customer and in accordance with this Agreement and the Company's privacy policy. The Customer acknowledges and agrees that the Company and the AI Providers may use the Customer Data to improve, enhance, or modify the Service or the AI services, or to develop new products or services, and that the Company and the AI Providers may retain, aggregate, or anonymize the Customer Data for these purposes. The Customer also acknowledges and agrees that the Company and the AI Providers may disclose the Customer Data to comply with any legal obligations, requests, or orders, or to protect the rights or interests of the Company, the AI Providers, or any third parties. The Customer is solely responsible for the security, backup, and integrity of the Customer Data, and for ensuring that the Customer Data is accurate, complete, and up-to-date. The Company and the AI Providers are not liable for any loss, damage, or corruption of the Customer Data, or any unauthorized access, use, or disclosure of the Customer Data, unless caused by the Company's or the AI Providers' gross negligence or willful misconduct. All customer data once ingested is encrypted both during transit and at rest.

4. Fees and payment

The Customer agrees to pay the fees for the Service as specified by the Company, in accordance with the payment terms and methods provided by the Company. The fees are exclusive of any taxes, duties, or charges that may be applicable to the Service, and the Customer is responsible for paying any such taxes, duties, or charges, except for those based on the Company's income. The fees are non-refundable, unless otherwise agreed by the Company in writing. The Company may change the fees at any time, upon a prior notice to the Customer, and the Customer's continued use of the Service after the effective date of the change constitutes the Customer's acceptance of the new fees. The Company may suspend or terminate the Customer's access to the Service if the Customer fails to pay the fees when due, or if the Customer's payment method is invalid, expired, or declined.

5. Term and termination

5.1 Term. This Agreement shall commence on the Effective Date and shall continue in full force and effect for a period of [insert duration], unless earlier terminated in accordance with the provisions of this Agreement.

5.2 Termination for Convenience. Either Party may terminate this Agreement for any reason, or no reason, by providing the other Party with 60 days' written notice.

5.3 Termination for Cause: Either Party may terminate this Agreement immediately upon written notice to the other Party if the other Party:

Materially breaches any provision of this Agreement and fails to cure such breach within [insert number] days after receiving written notice of the breach. Becomes insolvent, files for bankruptcy, or has a receiver appointed for its assets. Effect of Termination: Upon termination of this Agreement for any reason: All rights and obligations of the Parties under this Agreement shall cease, except for those rights and obligations that expressly survive termination. Each Party shall return or destroy all Confidential Information of the other Party in its possession. Survival: The provisions of this Agreement that by their nature are intended to survive termination or expiration shall so survive, including but not limited to [insert specific sections, e.g., confidentiality, indemnification, etc.].

6. Confidentiality

The Customer agrees to keep confidential and not to disclose, use, or exploit any confidential or proprietary information of the Company that the Customer receives or accesses through the Service, such as trade secrets, inventions, business plans, financial data, customer data, marketing data, or other information that is not publicly known or readily ascertainable, and that is valuable to the Company and their business (the "Confidential Information"). The Customer also agrees to protect the Confidential Information from unauthorized access, use, or disclosure by any third parties, using at least the same degree of care that the Customer uses to protect the Customer's own confidential information of a similar nature, but in no event less than a reasonable degree of care. The Customer further agrees to return or destroy all Confidential Information in the Customer's possession or control, including any copies, reproductions, summaries, notes, or analyses, upon the termination of this Agreement or upon the request of the Company or the AI Providers. The obligation of confidentiality does not apply to any Confidential Information that:

Was already known to the Customer prior to receiving it from the Company or the AI Providers, as evidenced by written records.

Was independently developed by the Customer without reference to or reliance on the Confidential Information, as evidenced by written records.

Was lawfully obtained by the Customer from a third party who had the right to disclose it and who was not under a confidentiality obligation to the Company or the AI Providers.

Became publicly available through no fault or breach of the Customer.

Was required to be disclosed by law, regulation, court order, or governmental authority, provided that the Customer gives the Company or the AI Providers prior notice and reasonable assistance to obtain a protective order or limit the scope of disclosure.

7. Intellectual property

The Customer acknowledges and agrees that the Company and its licensors own and retain all rights, title, and interest in and to the Service and any results generated by the Service, including any patents, trademarks, trade names, trade dress, logos, slogans, domain names, and copyrights, and any other intellectual property rights or proprietary rights that may arise from or relate to the Service or the results (the "Company IP"). The Customer also acknowledges and agrees that the AI Providers and their licensors own and retain all rights, title, and interest in and to the AI services and any results generated by the AI services, including any intellectual property rights or proprietary rights that may arise from or relate to the AI services or the results (the "AI Provider IP"). Nothing in this Agreement grants or transfers to the Customer any ownership or license rights in or to the Company IP or the AI Provider IP, except for the limited license to access and use the Service as expressly provided in this Agreement.

8. Changes to this Terms of service

We retain the right to modify this document to align with new regulations, legal precedents, and evolving industrial or commercial practices.

If any changes are made to our Terms of service, they will be published on this page. The last modification to this document occurred on 01/07/2024.

9. Contact us

If you have any questions about this document, please contact us at security@lightenup.ai. We are committed to protecting your privacy and ensuring your data is handled with the utmost care.

Exhibit F:

PRIVACY POLICY

This privacy policy (the "Policy") explains how LIGHTNEUP AI SERVICES (the "Company"), collects, uses, shares, and protects the personal data of the customers (the "Customers") who access and use the Company's software-as-a-service (Saas) application programming interface (API) offering (the "Service"). The Service leverages various artificial intelligence (AI) services provided by third party AI providers, such as OpenAI, Azure OpenAI, and Amazon AWS Bedrock (the "AI Providers").

1. What personal data do we collect and why?

We collect the following types of personal data from the Customers or through the Service:

Account data: We collect the Customers' name and surname when they log in to the Service. We use this data to identify, authenticate, and communicate with the Customers, and to provide and manage the Service.

Service data: We collect the data, content, and information that the Customers submit, upload, or transmit to the Service or the AI Provider, or that the Service or the AI Provider collect, process, or store on behalf of the Customers (the "Service Data"). The Service Data may include text, images, audio, video, or other types of data that the Customers use or generate through the Service or the AI services. We use this data to provide and improve the Service and the AI services, and to comply with the Customers' instructions and requests. The Customers are solely responsible for the Service Data, and they should ensure that they have the necessary rights and permissions to use and share the Service Data, and that the Service Data does not infringe or violate the rights or interests of the Company, the AI Provider, or any third parties, or any applicable laws or regulations.

Usage data: We collect the data about how the Customers access and use the Service or the AI services, such as the IP address, device type, browser type, operating system, language preference, time zone, location, referral source, pages visited, actions taken, errors encountered, and other technical and behavioral data. We use this data to monitor and analyze the performance, functionality, and usage of the Service and the AI services, and to improve and personalize the Customer experience.

2. How do we share the personal data?

We may share the personal data with the following parties and for the following purposes:

AI Provider: We share the Service Data with the AI Provider, as necessary to provide the Service and the AI services to the Customers, and in accordance with the Customers' instructions and requests. The AI Provider may use the Service Data to improve, enhance, or modify the AI services, or to develop new products or services, and they may retain, aggregate, or anonymize the Service Data for these purposes. The AI Provider may also disclose the Service Data to comply with any legal obligations, requests, or orders, or to protect the rights or interests of the AI Provider or any third parties. The Customers should review the privacy policies of the AI Provider before accessing or using the AI services. Our AI provider privacy policies are attached for reference below.

Azure

Service Providers: We share the personal data with our service providers, such as hosting providers, payment processors, analytics providers, marketing providers, or other third parties that help us to provide and improve the Service. We only share the personal data that is necessary for the service providers to perform their services, and we require them to protect the personal data and use it only for the purposes that we authorize.

Affiliates: We share the personal data with our affiliates, such as our parent company, subsidiaries, or other related entities, for the purposes of providing and improving the Service, and for marketing and advertising purposes, subject to the Customers' consent and preferences.

Business Partners: We share the personal data with our business partners, such as our resellers, distributors, or other third parties that offer or promote the Service, subject to the Customers' consent and preferences. The Customers should review the privacy policies of these business partners before accessing or using their products or services.

Business Transfers: We may share the personal data with a successor entity in the event of a merger, acquisition, reorganization, sale of assets, or bankruptcy, or with a potential buyer or investor in the course of a due diligence process. We will notify the Customers of any change of ownership or control of the personal data, and we will ensure that the personal data is transferred and used in accordance with this Policy and the applicable laws and regulations.

Legal and Regulatory Compliance: We may share the personal data with the competent authorities, such as courts, regulators, or law enforcement agencies, if we are required or permitted to do so by law, regulation, court order, or governmental request, or if we believe that such disclosure is necessary or appropriate to protect the rights or interests of the Company, the AI Provider, or any third parties, or to prevent or investigate any illegal, fraudulent, or harmful activities.

3. How do we protect personal data?

We take reasonable and appropriate measures to protect the personal data from unauthorized access, use, or disclosure, such as encryption, access controls, and security audits. However, we cannot guarantee that the personal data is completely secure or immune from any cyberattacks, breaches, or errors, and we disclaim any liability for any loss, damage, or corruption of the personal data, unless caused by our gross negligence or willful misconduct. The Customers are responsible for maintaining the security and confidentiality of their account credentials, managing access to these accounts and devices, and for notifying us promptly of any unauthorized or suspicious activities on their account or the Service.

4. How long do we keep the personal data?

We retain the personal data for as long as necessary to provide and improve the Service and the AI services, and to comply with our legal obligations, contractual agreements, and business policies. We may delete or anonymize the personal data when it is no longer needed for these purposes, or when the Customers request us to do so, subject to our retention rights and obligations under the applicable laws and regulations.

5. What rights do the Customers have?

The Customers have the following rights with respect to their personal data, subject to the applicable laws and regulations, and our legitimate interests and obligations:

Access: The Customers have the right to access and obtain a copy of their personal data that we hold and process, and to verify the accuracy and completeness of their personal data.

Correction: The Customers have the right to correct or update their personal data that is inaccurate, incomplete, or outdated, or to request us to do so.

Deletion: The Customers have the right to delete or request us to delete their personal data that is no longer necessary for the purposes that we collected or processed it, or that we processed unlawfully or without their consent, or that they withdraw their consent to.

Restriction: The Customers have the right to restrict or request us to restrict the processing of their personal data, if they contest the accuracy or lawfulness of their personal data, or if they object to the processing of their personal data for our legitimate interests or direct marketing purposes.

Objection: The Customers have the right to object or request us to stop the processing of their personal data for our legitimate interests or direct marketing purposes, unless we demonstrate compelling and overriding grounds for the processing, or for the establishment, exercise, or defense of legal claims.

Portability: The Customers have the right to receive or request us to transmit their personal data that they provided to us, in a structured, commonly used, and machine-readable format, and to transfer their personal data to another data controller, without hindrance from us, where technically feasible, and where the processing is based on their consent or a contract, and is carried out by automated means.

Withdrawal of consent: The Customers have the right to withdraw their consent to the processing of their personal data at any time, without affecting the lawfulness of the processing based on their consent before the withdrawal, and without prejudice to the processing based on other lawful grounds.

Complaint: The Customers have the right to lodge a complaint with the relevant data protection authority, if they believe that we have violated their rights or interests, or any applicable laws or regulations.

6. Changes to this Privacy Policy

We retain the right to modify this policy to align with new regulations, legal precedents, and evolving industrial or commercial practices.

If any changes are made to our Privacy Policy, they will be published on this page. The last modification to this Privacy Policy occurred on 01/07/2024.

12. Contact Us

If you have any questions about this Privacy Policy compliance or how we handle your data, please contact us at security@lightenup.ai. We are committed to protecting your privacy and ensuring your data is handled with the utmost care.

* Signature required