Information Security Exhibit

INFORMATION SECURITY EXHIBIT Security and privacy sit at the core of product development at LIGHTENUP AI SERVICES LTD. (hereinafter, “lightenUp”). 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, and the collection of documents and policies made available and amended by lightenUp from time to time on the Trust Portal.
● “Cloud Solution” means the Solution as a service provided to the Customer.
● “Customer” means the entity using paid Software and/or Services under an Service Order 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 on the Trust Portal.
● “On-Premise Solution” means Solution deployed on Customer premises.
● “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” or “On-Premise 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 client.

● “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.

1. 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.

2. PRODUCT SECURITY

2.1 Product Development Practices

2.1.1. 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.

2.1.2.lightenUp shall document change control decisions and procedures to manage changes to software, supporting infrastructure and facilities throughout each component’s lifecycle. Prior to implementing any changes, lightenUp shall (1) establish acceptance criteria for production change approval and implementation; and (2) require stakeholder approval prior to change implementation as applicable.

2.1.3. 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.

2.1.4. Furthermore, lightenUp shall limit and audit staff access to the software's source code. It's also mandatory for developers to participate in training sessions on secure system development on a regular basis.

2.2. Cryptographic Controls

2.2.1. Encryption is a crucial element of lightenUp's security approach, designed to safeguard information from unauthorized access. All customer data stored within the software is encrypted. Whether it's being transmitted, in transit, over the internet or within lightenUp's internal service components, at rest, customer data is always securely transferred and stored.
2.2.3. The Customer Data is encrypted to increase data protection and to fulfill compliance requirements for encryption at rest. A symmetric encryption key is used to encrypt and decrypt the data accessed at runtime.
2.2.4 Customer Data transferred into or out of lightenUp's Services is encrypted in transit using Layer/Transport Layer Security (SSL/TLS) certificates. All the supported protocols, Websocket and Rest, are implemented with TLS 1.2+. 2.3. Network Security and Segregation
2.3.1 A WAF solution is implemented to provide protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. 2.3.2 Test, development and production environments per tenant are fully physically segregated across multiple zones to ensure security, compliance with Data privacy policies and high-availability.
2.3.4 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.

2.4. Access Controls

2.4.1 Programmatic access is allowed using OAuth2 authentication and authorization protocols with JWT Tokens. LightenUp Solutions leverages an external identity provider, AWS Cognito, to manage JWT tokens and validate the identity of incoming requests. 2.5. Access to Customer Data
2.5.1. lightenUp core product, AIVA, 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.

2.6. Customer Data Back-ups

2.6.1. Regular back-ups of Customer Data in Cloud Software are performed automatically by lightenUp underlying infrastructure as a service/platform as a service ("IaaS/PaaS") provider. Each backup is stored in multiple locations to ensure resiliency.
2.6.2. Upon request, available backup records stored by lightenUp to review any record of system activity related to Customer Data.

2.7. Customer Data Retention

2.7.1. 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.

2.8. Logs Information

2.8.1. Logging capabilities are built into the Software, which the Customer can enable to capture informational events, error, and warning messages relevant to the application as well as audit trails for actions performed. Details can be found in the Documentation. 2.8.2. lightenUp enables operational logs and security logs of activity in Cloud Software. Operational logs are used for monitoring uptime and availability of infrastructure and Cloud Software. Security logs are used for identifying security incidents, policy 2 violations, fraudulent activity, auditing, and forensic analysis, supporting investigations, establishing baselines, and identifying trends and potential long-term problems. 2.8.3. lightenUp shall generate administrator and event logs for systems and applications that store, allow access to, or process Customer Data. The administrator and event logs shall be archived for a minimum of one hundred eighty (180) calendar days;

2.9 Personal Data Protection

2.9.1. lightenUp takes Personal Data protection very seriously and encourages Customers to minimize the use of Personal Data with Cloud Software, in line with the principles of the applicable legislation. Further rights and obligations between lightenUp and Customer with respect to protection of Personal Data as part of Customer Data will be governed by appropriate data protection agreements executed between the Parties in accordance with GDPR and any applicable legislation. 2.9.2. Though lightenUp is committed to making its operating environment as compliant as possible, some Software components might not

meet all standards required by industry standards such as PCI DSS, or HIPAA. lightenUp expressly prohibits Customers from using CHD, SAD, PHI, or any other specifically regulated personally identifiable information with Cloud Software, except where lightenUp has expressly instructed otherwise in the agreement, or by updates to this Exhibit or the Trust Portal. Nonetheless, the Customer is ultimately responsible in deciding whether the Software can be used in accordance with the laws, rules, and regulations applicable to Customer's operations.
2.9.3. lightenUp, in its capacity as data controller, makes available a process for data subject access requests, as required by the GDPR, available on the Trust Portal. lightenUp will notify the Customer without undue delay of any data subject requests which lightenUp in its capacity as data processor may receive but to which the Customer in its capacity as data controller must respond.
2.9.4. As a controller, lightenUp processes Personal Data in accordance with its Privacy Policy available on the Trust Portal. 2.10. Malware 2.0.1. lightenUp conducts routine tests of both proprietary and third-party code incorporated in the Software. 2.10.2. lightenUp implements, sustains, and refreshes anti-malware defenses within its operational environment and on business computing assets. 2.11. Vulnerabilities Management
2.11.1. 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. 2.11.2. Regular testing is conducted to detect vulnerabilities in the Software and its associated ecosystem to safeguard Customers' usage of the Software from harmful activities. 2.11.3. 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. 3. INTERNAL SECURITY PRACTICES

3.1. Access Controls

3.1.1. 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.
3.1.2. 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.

3.1.3. 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. 3
3.1.4. 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.
3.1.5. Access to business systems and applications shall be based on the principles of least privilege and segregation of responsibilities.
3.1.6. 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.

3.2. Risk Management

3.2.1. lightenUp has established a risk management procedure aimed at minimizing risks to a tolerable level. Risk evaluations are performed regularly and identified risks are addressed based on their severity and business priorities.

3.3. Physical Security

3.3.1. Physical security measures are enforced to discourage unauthorized access or harm caused by physical or environmental threats, safeguarding LightenUp employees, facilities, system and network devices, and information, as well as preventing disruptions to organizational operations. The level of security measures, policies, and procedures implemented conforms to the legal, regulatory, or contractual obligations linked to each facility upon its establishment and readiness to handle business services.
3.3.2. lightenUp enforces a clean desk and clean screen policy. The purpose of this policy is to establish the minimum requirements for maintaining a “clean desk”, where sensitive/confidential information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight.

3.4. Asset Management

3.4.1. 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.
3.4.2. 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. Employees are required to return all equipment upon termination of employment.
3.4.3. 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

3.5.1. 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.
3.5.2. lightenUp maintains policies in place restricting the storage of Customer Data locally, on the employees' devices or on removable media.

3.6. Mobile Devices and Teleworking

3.6.1. lightenUp has established comprehensive policies regarding teleworking and the handling of Customer Data from remote devices. Devices provided by the company that have access to Customer Data are appropriately safeguarded.
3.6.2. lightenUp implements various security measures on employee devices, including: a) Enforcing a multi-factor authentication access control mechanism to grant full access to Customer Data. b) Regularly applying security patches to applications and system software. 4 c) Requiring authorization for business applications before they can access Customer Data.

3.7. Human Resources Security

3.7.1. lightenUp may conduct background checks prior to employment, always in compliance with relevant laws.
3.7.2. 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.

3.7.3. 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.

3.8. Vendor Risk Management

3.8.1. 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.
3.8.2. 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 sub-contractors as the ones applicable to lightenUp.
3.8.3. lightenUp strives to maintain the right to perform audits to monitor the compliance of its sub-contractors with the agreed technical and organizational measures regarding data confidentiality and security.

4. INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

4.1. 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.
4.2. 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.
4.3. Incident responders meticulously analyze incident root causes, integrate lessons learned into the incident management system, and propose continuous enhancements to system and data integrity.
4.4. 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.
4.5. As part of lightenUp's commitment to incident management, lightenUp will establish and uphold a formally documented incident management policy. This policy will encompass mechanisms for reporting actual incidents affecting the security of Customer Data, including unauthorized access or disclosure. Additionally, it will outline procedures for

notifying relevant authorities in accordance with applicable law and customer requirements, as well as protocols for forensic investigation of security incidents.
4.6. 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.

5. AWARENESS AND TRAINING

5.1. lightenUp conducts an annual 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.
5.2. lightenUp provides information security training to employees upon hiring and regularly thereafter. 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.

6. POLICY MONITORING, TESTING AND REVIEWING

6.1. lightenUp conducts policy reviews on an annual basis and adjusts them as necessary to align with evolving legal requirements, prevailing industry standards, internal organizational practices, and contractual commitments. These updates ensure that policies remain relevant and suitable for addressing the risks encountered by lightenUp.

7. CUSTOMER ASSESSMENT

7.1. 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 this page. The last modification to this document occurred on 05/03/2026.

CONTACT US If you have any questions about this Information Security Exhibit, please contact us at legal@aiva.build.