

SECURITY ADDENDUM

This SECURITY ADDENDUM (the “**Addendum**”) forms part of and is incorporated into the TECHNOLOGY ACCESS TERMS to which it is attached (the “**Terms**”). Capitalized terms used but not defined herein shall have the meanings set forth in the Terms. This Addendum is effective as of the Effective Date set forth in the Agreement.

1. **Information Security Program.** Eudia shall implement, maintain, and comply with information security policies and procedures designed to protect the confidentiality, integrity, and availability of Confidential Information provided or made available to Eudia by or on behalf of Customer in connection with the Agreement (“**Customer Data**”) and any systems that store or otherwise process it, which are: (a) aligned with an industry-standard control framework (e.g., NIST SP 800-53, ISO 27001, CIS Critical Security Controls); (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Customer Data.
2. **Risk Assessment.** Eudia shall maintain risk assessment procedures for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance with the organization’s policies and procedures and reporting the condition of the organization’s information security and compliance to internal senior management.
3. **Personnel Training.** Eudia shall train personnel to maintain the confidentiality, integrity, and availability of Customer Data, consistent with the Terms and applicable laws.
4. **Vendor Management.** Eudia shall, prior to engaging Subprocessors and other subcontractors, conduct reasonable due diligence and monitoring to ensure subcontractors are capable of maintaining the confidentiality, integrity, and availability of Customer Data.
5. **Access Controls.** Only authorized personnel and third parties are permitted to access Customer Data. Eudia shall maintain logical access controls designed to limit access to Customer Data and relevant information systems (e.g., granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking or changing access when employment terminates or changes in job functions occur).
6. **Secure User Authentication.** Eudia shall maintain password controls designed to manage and control password strength, expiration, and usage. These controls include prohibiting users from sharing passwords and requiring that passwords controlling access to Customer Data must: (a) be at least 8 characters in length and meet minimum complexity requirements; (b) not be stored in readable format on the organization’s computer systems; (c) have a history threshold to prevent reuse of recent passwords; and (d) if newly issued, be changed after first use.
7. **Incident Detection and Response.** Eudia shall maintain policies and procedures to detect and respond to any actual or reasonably suspected alteration, acquisition, disclosure of, or access to Customer Data (“**Security Incidents**”) and encourage the reporting of such Security Incidents.
8. **Encryption.** Eudia shall apply industry standard encryption to Customer Data: (a) stored on any medium (i.e., laptops, mobile devices, portable storage devices, file servers and application databases); and (b) transmitted across any public network (such as the Internet) or wirelessly.
9. **Network Security.** Eudia shall implement network security controls such as up-to-date firewalls, layered DMZs, updated intrusion detection and prevention systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
10. **Vulnerability Management.** Eudia shall detect, assess, mitigate, remove, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code, by implementing vulnerability management, threat protection technologies, and scheduled monitoring procedures.
11. **Change Control.** Eudia shall follow change management procedures and implement tracking mechanisms designed to test, approve, and monitor all changes to the organization’s technology and information assets.
12. **Physical Security.** Eudia utilizes Microsoft Azure and Amazon Web Services cloud hosting infrastructure. Eudia shall periodically review the applicable security and compliance reports of its existing cloud hosting providers, and any cloud hosting providers to which Eudia transfers Customer Data, to ensure that they have taken steps to ensure the physical and environmental security of data centers, server room facilities and other areas containing Customer Data.
13. **Business Continuity and Disaster Recovery.** Eudia shall maintain business continuity and disaster recovery policies and procedures designed to maintain service and recover from foreseeable emergency situations or disasters.