ABACUS ACCEPTABLE USE POLICY

Last Updated: 2024-11-10

This Acceptable Use Policy forms part of the *Master Professional Services Agreement* ("Principal Agreement") between: (i) for US based "Client": **ABACUS INFORMATION TECHNOLOGY, LLC (d/b/a Abacus Group LLC)**; or for UK based "Client": **ABACUS INFORMATION TECHNOLOGY UK LIMITED** (*collectively* "**Abacus**") acting on its own behalf and as agent for each Abacus Affiliate; and (ii) "**CLIENT"** *(as detailed in the respective Principal Agreement)* acting on its own behalf and as agent for each Client Affiliate.

The terms used herein shall have the meanings as set forth herein. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement. Except where the context requires otherwise, references herein to the Principal Agreement are to the Principal Agreement as amended by, and including, this addendum.

This Acceptable Use Policy (this *"Policy"*), effective as of the Effective Date, governs Client's use of Abacus's Products and Services. Client agrees that it is responsible for ensuring that all of its Authorized Users comply with this Policy. Capitalized terms used herein and not otherwise defined herein have the meanings ascribed to such terms elsewhere in the Principal Agreement.

1. No Unauthorized Access. Client agrees that its Authorized Users shall: (i) access only those Products and Services that have been authorized by Abacus; and (ii) use such Products and Services only in the manner specifically authorized by Abacus in the Agreement and any applicable SOW. Client's Authorized Users shall not access or attempt to access any of the Products or Services through any application, web portal, application programming interface *("API")*, or other means that has not been specifically authorized by Abacus. Client's Authorized Users shall not access or attempt to access any file, communication, or other data of any other person unless such access has been expressly authorized by Client and Abacus. Client's Authorized Users shall not attempt to exceed any limitations on the use of the Products and Services, including storage and volume limitations that may be imposed by Abacus pursuant to the Agreement or any applicable SOW.

2. No Sharing Credentials. Notwithstanding credentials shared with an authorized Abacus representative for the purposes of troubleshooting, Client's Authorized Users shall not: (i) share their credentials used to access the Products or Services with any other person; (ii) access the Products or Services with the credentials of any other user; or (iii) permit any other person to access the Products or Services using their credentials.

3. No Unauthorized Devices. Client agrees that its Authorized Users shall access the Products and Services only from personal computers, tablets, mobile phones, or other computing devices (collectively *"Devices"*) that meet such security standards as may be established from time to time by Client and Abacus.

4. No Installing Software. Client further agrees that its Authorized Users shall not install or cause to be installed any software on any device that connects to the Products or Services without the prior written consent of Abacus.

5. No Interfering with the Services. Client's Authorized Users shall not use any of the Products or Services in any manner that: (i) interferes with any other person's use of the Products or Services; or (ii) adversely impacts the availability, stability, or reliability of any of the Products or Services. This prohibition includes, but is not limited to: (a) conducting or facilitating denial of service attacks; (b) operating open proxies, open mail relays, or recursive domain name servers; (c) monitoring or crawling of a system in a manner that negatively affects the system; (d) introducing viruses or other

malicious software to the Products or Services; or (e) blocking or otherwise interfering with the installation of security patches or other software updates required by Abacus.

6. No Unauthorized Security Testing or Monitoring. Client's Authorized Users shall not engage in any of the following activities: (i) penetration testing of any of the Products or Services; (ii) reverse engineering of any of the Products or Services; (iii) probing of any of the Products or Services; (iv) port sniffing any of the Products or Services; or (v) any other security testing of the Products or Services, in each case without the prior written consent of Abacus. Client's Authorized Users shall not intercept or monitor traffic on the network on which the Products or Services are hosted without the written permission of Abacus.

7. No Security Violations. Client's Authorized Users shall not use the Products or Services to violate the security or integrity of any computer, mobile device, computing device, network, communications system, or software application.

8. No Unsolicited Bulk or Misleading Communications. Client's Authorized Users shall not use the Products or Services to: (i) send unsolicited bulk electronic communications (commonly referred to as "spam") including, but not limited to electronic mail, instant messaging, and social media postings; (ii) where applicable to the Products and/or Services, violate the federal CAN-SPAM Act through use of falsified or misleading header information, deceptive subject lines, or otherwise; or (iii) assume a sender's identity without the sender's explicit permission.

9. Deceptive and Fraudulent Content. Client's Authorized Users shall not use the Products or Services in any deceptive or fraudulent manner or for any fraudulent purposes including, but not limited to: (i) attempting to obtain information from third parties under false pretenses (commonly referred to as "phishing"); or (ii) promoting or offering for purchase fraudulent goods or services.

10. No Hosting. Notwithstanding applications, websites, databases, or software that has been specifically contracted to be hosted by Abacus, Client's Authorized Users shall not host or install any application, website, database, or software on the Products or Services, without the prior written consent of Abacus.

11. Intellectual Property. Client's Authorized Users shall not use the Products or Services to infringe upon the intellectual property rights of any person or entity, including, but not limited to, copyrights, trademarks, patents, and trade secrets. This prohibition includes, but is not limited to: (i) using unlicensed software; (ii) violating the terms of a software license; and (iii) the unauthorized downloading or streaming of copyrighted material. Abacus reserves the right to remove or disable access to any material a content owner alleges infringes upon their intellectual property rights upon receiving a notice that substantially complies with the Digital Millennium Copyright Act or other equivalent local law or regulation.

12. No Harassment. Client's Authorized Users shall not use the Products or Services to host, post, transmit, or re-transmit any content that harasses, intimidates, defames, or threatens the health or safety of any person.

13. Special Provisions for Voice Services. The Services may include the provision of voice communication services ("Voice Services"). Client shall not permit its Authorized Users to use the Voice Services to engage in harassment or violate any applicable law, including, but not limited to, laws governing telemarketing and the recording of phone conversations.

14. Export Violations. Portions of the Products or Services may be subject to restrictions on export under applicable law. Client's Authorized Users shall not export any portion of the Products or Services in violation of applicable law.

15. No Illegal Activity. Client's Authorized Users shall not use the Products or Services to violate any law that is applicable to Client or its Authorized Users. Abacus reserves the right to report any illegal activity of which it may become aware to law enforcement and to preserve evidence of any such activity.

16. Violations. Abacus retains the right, but not the obligation, to monitor Client's use of the Products and Services for compliance with the terms of this Policy and to investigate any suspected violation of this Policy. Client shall promptly notify Abacus in writing of any violations of this Policy of which it becomes aware. Client agrees to cooperate with Abacus in investigating any suspected violations of this Policy. Any material violation of this Policy shall be deemed to constitute a breach of the Agreement.

17. Remedies. Abacus has the right to take immediate actions to protect the Products and Services from any user or device that violates this Policy. These actions include, without limitation, deactivation or disconnection of any user or device.