MINDSTAND PRIVACY POLICY

Hi! This privacy policy sets out how MindStand Technologies **("MindStand")** uses and protects any information that you provide to MindStand. MindStand is devoted to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when accessing your account information, you can be assured that such information will only be used in accordance with this privacy statement. We do not share your non-public personal information with unaffiliated third parties. Information is only shared with your consent except for the specific purposes below, in accordance with all applicable laws. Please read this policy carefully. It gives you important information about how we handle your personal information. MindStand reserves the right to change this policy at any time.

USE OF INFORMATION

We limit the collection and use of non-public personal information to the minimum we believe is necessary to deliver superior service to you. **"Service"** means MindStand's internet-accessible service that provides use of MindStand's online harassment, hate speech, and other troubling behaviors detection and reporting software that is hosted and managed by MindStand and made available to Customer over a network on a term-use basis.

Confidentiality.

Definition of Confidential Information. During the course of performance under this Agreement, each party may make available to the other party information that is not generally known to the public and at the time of disclosure is either identified as, or should reasonably be understood by the receiving party to be, proprietary or confidential (the "**Confidential Information**"). Confidential Information specifically includes this Agreement, the Service, Order Form(s), Customer Data, Results (as defined below), business plans, product plans and roadmaps, strategies, forecasts, projects and analyses, financial information and fee structures, business processes, methods and models, and technical documentation. Confidential Information does not include information that: (a) is or becomes publicly available without breach of this Agreement by the receiving party; (b) was known to the receiving party prior to its disclosure by the disclosing party; (c) is or was independently developed by the receiving party without the use of any Confidential Information of the disclosing party; or (d) is or was lawfully received by the receiving party from a third party under no obligation of confidentiality.

Protection of Confidential Information. Except as otherwise expressly permitted under this Agreement, with the express prior written consent of the disclosing party, or as required by law, the receiving party will not disclose, transmit, or otherwise disseminate to a third party any Confidential Information of the disclosing party. The receiving party will use the same care and discretion with respect to the Confidential Information received from the disclosing party as it uses with its own similar information, but in no event less than a reasonable degree of care. The receiving party may disclose the disclosing party's Confidential Information to its employees, Affiliates, consultants, subcontractors, agents, or advisors ("Representatives") who have a strict need to know such Confidential Information for the purpose of performing under this Agreement and only to those who are obligated to maintain the confidentiality of such Confidential

Information upon terms at least as protective as those contained in this Agreement. Either party may disclose the terms of this Agreement to potential parties to a bona fide fundraising, acquisition or similar transaction solely for purposes of the proposed transaction, provided that any such potential party is subject to written non-disclosure obligations and limitations on use no less protective than those set forth herein.

Equitable Relief. The receiving party acknowledges that the remedy at law for breach of this Section 6 may be inadequate and that, in addition to any other remedy the disclosing party may have, it shall be entitled to seek equitable relief, including, without limitation, an injunction or injunctions (without the requirement of posting a bond, other security or any similar requirement or proving any actual damages), to prevent breaches or threatened breaches of this Section 6 by the receiving party or any of its Representatives and to enforce the terms and provisions of this Section 6 in addition to any other remedy to which the disclosing party is entitled at law or in equity.

Compelled Disclosure. The receiving party may access and disclose Confidential Information of the disclosing party if legally required to do so in connection with any legal or regulatory proceeding; provided, however, that in such event the receiving party will, if lawfully permitted to do so, notify the disclosing party within a reasonable time prior to such access or disclosure so as to allow the disclosing party an opportunity to seek appropriate protective measures. If the receiving party is compelled by law to access or disclose the disclosing party's Confidential Information as part of a civil proceeding to which the disclosing party is a party, the disclosing party will reimburse the receiving party for its reasonable cost of compiling and providing secure access to such Confidential Information. Receiving party will furnish only that portion of the Confidential Information that is legally required to be disclosed, and any Confidential Information so disclosed shall maintain its confidentiality protection for all purposes other than such legally compelled disclosure.

Sensitive/Personal Information. Customer agrees that it shall not use the Service to send or store personal information subject to special regulatory or contractual handling requirements (e.g., Payment Card Industry Data Security Standards, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and any similar data protection laws) including without limitation: credit card information, credit card numbers and magnetic stripe information, social security numbers, driver's license numbers, passport numbers, government issued identification numbers, health-related information, biometric data, financial account information, personally identifiable information collected from children under the age of 13 or from online services directed toward children, and real time geo-location data which can identify an individual, or information deemed "sensitive" under applicable law (such as racial or ethnic origin, political opinions, or religious or philosophical beliefs).

DISCLOSURE

MindStand does not disclose any kind of non-public personal information about our customers to anyone, except when we believe it necessary for the conduct of our business, or where disclosure is required by law. Except in those specific, limited situations, without your consent, we will not make any disclosures of non-public personal information to other companies who may want to sell their products or services to you.

SECURITY

MindStand is committed to ensuring that your information is secure. In ensuring that your information is secure MindStand has instilled the following data security methods:

1. **Data Centers**. MindStand uses Microsoft Azure (Azure) to provide management and hosting of production servers and databases. Azure employs a robust physical security program with multiple certifications, including SSAE 16 and ISO 270001 certification.

2. **Access, Controls, and Policies**. Access to manage MindStand's Azure environment requires multi-factor authentication and access to Customer Data is restricted to a limited set of approved MindStand employees. Azure networking features such as security groups are leveraged to restrict access to Azure instances and resources and are configured to restrict access using the principle of least privilege. Employees are trained on documented information security and privacy procedures. Every MindStand employee signs an NDA that binds them to the terms of MindStand's data confidentiality policies and access to MindStand systems is promptly revoked upon termination of employment.

MindStand will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so.