

ADDENDUM 2

ACCEPTABLE USE POLICY

Effective Date: 02nd January 2022

1. Introduction

- 1.1 This Acceptable Use Policy (the "AUP") applies to Customer's use of all of Provider's services, including all subscriptions for Provider's hosted software as a service solutions and any other related services that Provider may provide to Customer.
- 1.2 This AUP is incorporated by reference into, and governed by the Software as a Service Agreement between Provider and Customer.
- 1.3 Capitalized terms used below but not defined in this AUP have the meaning set forth in the Terms of Service or the Software as a Service Agreement.
- 1.4 Customer acknowledges that Provider does not actively monitor the content or the use of the Services.

2 Effective Date, Changes to Policy

- 2.1 **Effective Date:** This AUP is current as of the date set forth above. Provider reserves the right to modify this AUP at any time by posting a revised version. Any changes will be effective as of the date Provider notifies Customer of the revised version through email, or as otherwise specified in the AUP. By continuing to use the Service or access Customer's Account after a modified version of the AUP has been received, Customer agrees to comply with the latest version of the AUP. In the event of a conflict between the AUP and the Terms of Services, the Terms of Service will take precedence.

3. General usage rules

- 3.1 Customer must not use the SaaS and/or Services in any way that causes, or may cause, damage to the SaaS or the Services or impairment of the availability or accessibility of the SaaS and/or Services.
- 3.2 Customer must not use the SaaS and/or Services:
 - (a) in any way that is unlawful, illegal, fraudulent, deceptive or harmful; or
 - (b) in connection with any unlawful, illegal, fraudulent, deceptive or harmful purpose or activity.

4. Violations

- 4.1 Any violation of this AUP will be considered a material breach of Software as a Service agreement and/or any other agreement Customer has with Provider governing

Customer's use of the SaaS and/or Services. In addition to any other remedies that may be available to Provider, in case Provider suspects that any of Customer's activities, or use of the SaaS and/or Service, are in violation of this AUP, the Terms of Service SLA, SaaS Agreement or applicable Law, Provider may (i) remove such violating content, in whole or in part; and/or (ii) terminate or suspend Customer's Account/subscriptions or Customer's access to the SaaS and/or Service, with or without advance notice and without liability for Provider (including liability for any interruptions in services or other monetary loss related to enforcement to this AUP). The SaaS fees will usually not be refunded.

- 4.2 Customer will be solely responsible for any monetary damages suffered by Provider due to Customer's actions or inactions, including without limitation, regulatory penalties and punitive damages related to Provider's lost clients and revenues. Further, Customer agrees to indemnify and hold Provider harmless from and defend Provider against any third party or government claims, including all related damages, costs and expenses (including reasonable attorneys' fees), that arise due to Customer's violation this AUP, including damages related to other users of the SaaS and/or Services and attorney's fees.

5. Unlawful Content

- 5.1 Customer may not use SaaS and/or Services for storing, displaying, transmitting, distributing or otherwise processing illegal or harmful content. Content must not be illegal or unlawful, must not infringe any person's legal rights, and must not be capable of giving rise to legal action against any person (in each case in any jurisdiction and under any applicable law).

- 5.2 Content must not:

- (a) be libellous or maliciously false;
- (b) be obscene or indecent; attack or otherwise unlawfully relate to others based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability, or medical condition;
- (c) in any way target, exploit or abuse children 18 years of age or younger;
- (d) contain material advocating or advancing criminal hacking, cracking, or phishing;
- (e) infringe any copyright, moral right, database right, trade mark right, design right, right in passing off, or other intellectual property right;
- (f) infringe any right of confidence, right of privacy or right under data protection legislation;
- (g) contain material related in any way to illegal drugs or paraphernalia, marijuana and related paraphernalia, prescription drugs;
- (h) constitute negligent advice or contain any negligent statement;

- (i) constitute an incitement to commit a crime, instructions for the commission of a crime or the promotion of criminal activity;
 - (j) be in contempt of any court, or in breach of any court order;
 - (k) contain or consist of, and must not promote, distribute or execute by means of the SaaS and/or Services, any unlawful software and malicious code, (such as viruses, worms, time bombs, spyware, adware, Trojan horses and other harmful or malicious files, scripts, agents or programs, routines, applications or technologies), or corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
 - (l) constitute a breach of official secrets legislation; or
 - (m) constitute a breach of any contractual obligation owed to any person.
- 5.3 Customer must ensure that content is not and has never been the subject of any threatened or actual legal proceedings or other similar complaint.
- 5.4 Customer must not use the SaaS and/or Services to send any hostile communication or any communication intended to insult, including such communications directed at a particular person or group of people.

6. Unlawful Actions

- 6.1 Customer may not use the SaaS and/or Services to, nor allow its Users or any third-party to use the SaaS and/or Service to:
- (a) Publish, post, upload, distribute, promote, sell, support, facilitate or otherwise make available, or engage in any activity related in any way to, any Unlawful Content;
 - (b) Generate or facilitate unsolicited commercial email (spam), including without limitation:
 - sending communications or email in violation of any applicable anti-spam law or regulation;
 - sending unauthorized mail via open, third-party servers;
 - sending email to users who have requested to be removed from a mailing list;
 - marketing to any lists whose recipients did not express explicit consent to receive such marketing material;
 - selling to, exchanging with, sharing with or distributing to a third party personal information, including the email addresses of any person without such person's knowing and continued consent to such disclosure; or
 - sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no preexisting relationship;
 - (c) create a false identity for the purpose of misleading others, impersonate another person, entity or Provider (via the use of an email address or otherwise) or otherwise misrepresent the source of any communication;

- (d) conduct any security research or audit on Provider's systems, attempt to probe, scan or test the vulnerability of any Provider's system or network or breach any security or authentication measures without written permission to do so, including via scanners and automated tools, or perform significant load or security testing without first obtaining Provider's written consent, or otherwise interfere with other users' enjoyment of the SaaS and/or Services;
- (e) access or use any Provider's system or service without permission;
- (f) engage in activity in connection with illegal peer-to-peer file sharing;
- (g) remove any copyright, trademark or other proprietary rights notices contained in or on the SaaS and/or Services or reformat or frame any portion of the web pages that are part of the SaaS and/or Services;
- (h) obtain or attempt to obtain unauthorized access to, or materials or information from, the SaaS and/or any Services, accounts, computer systems or networks connected to any of the Services, including without limitation, through hacking, password mining or any other means;
- (i) violate in any manner the applicable guidelines published by any generally accepted industry associations, carrier guidelines or other industry, third party policies or requirements that Provider may communicate to Customer;
- (j) generate or facilitate any communications (including without limitation, SMS, MMS, or other text messages, calls, faxes, or push notifications) in violation of any applicable law including anti-spam, telemarketing or telephone consumer protection laws or regulations;
- (k) use, display, mirror or frame the SaaS and/or Services or any individual element within the Services, without Provider's express written consent;
- (l) access, tamper with, or use non-public areas of the SaaS and/or Services, Provider's computer systems, or the technical delivery systems of Provider's providers;
- (m) avoid, bypass, remove, deactivate, impair, descramble or otherwise circumvent any technological measure implemented by Provider or any of Provider's providers or any other third party (including another user) to protect the SaaS and/or Services;
- (n) attempt to disrupt or overwhelm Provider's infrastructure by imposing unreasonable requests or burdens on Provider's resources;
- (o) misuse or otherwise use the SaaS and/or Service in an excessive manner compared to the anticipated standard use (examined, at Provider's sole discretion), including without limitation, consuming a massive amount of storage or excessive use of bandwidth;
- (p) directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover or derive the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the SaaS and/or Services or any Provider's Technology; decrypt, modify, translate, or create derivative

works based on the SaaS and/or Services or any software (except to the extent expressly permitted by Provider); or remove any proprietary notices or labels;

(r) violate any other applicable laws or regulations.

- 6.2 Customer must not use the SaaS and/or Services to promote, host or operate any chain letters, Ponzi schemes, pyramid schemes, matrix programs, multi-level marketing schemes, "get rich quick" schemes or similar letters, schemes or programs.
- 6.3 Customer must not use the SaaS and/or Services in any way which is liable to result in the blacklisting of any of Provider's IP addresses.

7. Regulated Businesses

- 7.1 Customer must not use the SaaS and/or Services for any purpose relating to gambling, gaming, betting, lotteries, sweepstakes, prize competitions or any gambling-related activity.
- 7.2 Customer must not use the SaaS and/or Services for any purpose relating to the offering for sale, sale or distribution of drugs or pharmaceuticals.
- 7.3 Customer must not use the SaaS and/or Services for any purpose relating to the offering for sale, sale or distribution of knives, guns or other weapons.

8. Data mining

- 8.1 Customer must not conduct any systematic or automated data scraping, data mining, data extraction or data harvesting, or other systematic or automated data collection activity, by means of or in relation to the SaaS and/or Services.

9. Hyperlinks and Emails

- 9.1 Customer must not link to any material using or by means of the SaaS and/or Services that would, if it were made available through the SaaS and/or Services, breach the provisions of this Policy.
- 9.2 All e-mail messages sent using the SaaS and/or Services must use opt-out link, must include a valid physical address of the sender and must contain a clear subject line that does not mislead the recipient as to the contents of the e-mail.
- 10.4 Customer must publish, enforce and abide by a privacy policy that protects its clients' personal information in Customer's possession or under Customer's control.