ACCEPTABLE USE POLICY

This Acceptable Use Policy (the "AUP") sets out the rules that govern the use of services provided by Prosper IT, LLC, doing business as Endeavor IT ("Endeavor IT"). The AUP is part of the Agreement between Endeavor IT and Client and is incorporated into each Service Order by reference. Capitalized terms used in this AUP that are not defined herein have the meanings given in the MTC or the MSLA.

The AUP applies to Client and to every individual who accesses or uses any Service through Client, including Client's employees, contractors, agents, and other authorized users. Client is responsible for ensuring that its users comply with this AUP. Violation of this AUP may result in suspension or termination of affected Services, in addition to any other remedies available to Endeavor IT under the Agreement or applicable law.

1. Application

1.1 This AUP applies to all use of any Service provided by Endeavor IT, regardless of the manner of access. Each individual who accesses or uses a Service through Client is bound by this AUP, and any reference in this AUP to "Client" includes such individuals.

1.2 Client shall make this AUP available to its users and shall take reasonable steps to ensure compliance, including, where applicable, incorporating the substance of this AUP into Client's internal acceptable use policies, employee handbooks, and contractor agreements.

2. Prohibited Uses

Client shall not use any Service, and shall not permit any user to use any Service, in any of the following ways. The categories and examples below are illustrative; conduct of the same general character is prohibited even if not specifically listed.

2.1 Illegal Activity. Client shall not use the Services to engage in, facilitate, or attempt any conduct that violates applicable law, including:

(a) infringement of any copyright, trademark, patent, trade secret, or other intellectual property right;

(b) production, distribution, or solicitation of child sexual abuse material or any other content depicting the sexual exploitation of minors;

(c) illegal gambling, illegal drug distribution, illegal weapons trafficking, or other criminal activity;

(d) violation of economic sanctions administered by the U.S. Office of Foreign Assets Control (OFAC) or the export control laws of the United States;

(e) advocacy or facilitation of violence against any government, organization, group, individual, or property; and

(f) any other conduct that violates federal, state, or local law in any applicable jurisdiction.

2.2 Security Violations. Client shall not use the Services to compromise the security or integrity of any system, network, or account, including:

(a) accessing or attempting to access any system, network, account, or data without authorization, including by circumventing authentication or other security controls;

(b) scanning, probing, or testing the security of any system or network without authorization;

(c) introducing or distributing malware, including viruses, worms, ransomware, Trojan horses, spyware, or other malicious code;

(d) conducting or facilitating denial-of-service or distributed denial-of-service attacks;

(e) engaging in packet spoofing, forged routing information, deliberate overload of services, or attempts to crash any host or service; and

(f) exploiting any known or suspected vulnerability of any system, network, or account.

2.3 Abuse of Network Resources. Client shall not use the Services in a manner that abuses Endeavor IT's or any third party's network resources, including:

(a) sending unsolicited bulk messages (spam) by email, SMS, fax, voice, or other means;

(b) using deceptive, absent, or forged headers, sender identification, or routing information;

(c) evading or attempting to evade spam filters or content moderation systems;

(d) propagating chain letters, pyramid schemes, or similar mass communications;

(e) mining cryptocurrency on or through any Service or system managed by Endeavor IT, without Endeavor IT's prior written consent;

(f) operating or participating in a botnet, credential-stuffing operation, or similar coordinated automated abuse;

(g) connecting to or operating insecure devices, including unsecured Internet of Things devices, in a manner that exposes the Services or third-party systems to abuse; and

(h) using unauthorized automation in a manner that imposes disproportionate load on the Services or third-party systems.

2.4 Interference and Harm to Third Parties. Client shall not use the Services to interfere with or harm any other user or third party, including:

(a) flooding, jamming, or otherwise interfering with the operation of any system, network, or service;

(b) harassing, threatening, defaming, or stalking any person;

(c) publishing, distributing, or transmitting content that is obscene, lewd, or harmful to minors;

(d) falsifying identity or contact information, including impersonation of another person or entity; and

(e) publishing private information of another person without that person's authorization, including doxing.

2.5 Misuse of AI and Automation. Client shall not use any artificial intelligence or automated tools made available through the Services to:

(a) generate content for fraud, deception, harassment, or impersonation of another person or entity;

(b) produce or distribute deepfakes or synthetic media intended to mislead recipients about the identity, statements, or actions of a real person, without that person's authorization;

(c) scrape, harvest, or otherwise extract data from any third-party system in violation of that system's terms of service or applicable law; or

(d) generate or distribute spam, malware, or other content otherwise prohibited by this AUP.

3. Regulated Data

3.1 Client shall not store, process, or transmit any of the following categories of data using the Services unless and until the Parties have executed the corresponding Compliance Addendum:

(a) Protected Health Information, as defined in 45 CFR § 160.103, governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires a Business Associate Agreement;

(b) Cardholder Data, as defined by the Payment Card Industry Data Security Standard (PCI DSS), which requires a PCI Compliance Addendum; and

(c) Criminal Justice Information, as defined by the FBI Criminal Justice Information Services (CJIS) Security Policy, which requires a CJIS Security Addendum.

3.2 If Client introduces regulated data of any of the foregoing categories into a Service without the corresponding Compliance Addendum, Endeavor IT may suspend the affected Service immediately and without prior notice until the matter is resolved, in addition to all other rights and remedies under the Agreement.

4. Enforcement

4.1 Non-Emergency Violations. For AUP violations that do not constitute an emergency, Endeavor IT shall use commercially reasonable efforts to provide notice to Client and a reasonable opportunity to cure before suspending or terminating any Service.

4.2 Emergency Violations. Endeavor IT may suspend or terminate any affected Service immediately and without prior notice in response to any of the following:

(a) introduction of regulated data into a Service without the corresponding Compliance Addendum required by Section 3;

(b) an active security incident or threat to Endeavor IT systems, Client systems, or third-party systems originating from or affecting the Services;

(c) conduct constituting illegal activity under Section 2.1;

(d) conduct causing or threatening imminent harm to third parties; or

(e) receipt of a lawful order from a court, law enforcement agency, or government authority with jurisdiction.

4.3 Subcontractor and Vendor Action. Where a Subcontractor or Vendor takes action affecting the Services in response to an AUP violation, Endeavor IT shall make commercially reasonable efforts to notify Client and to mitigate the impact, but is not responsible for actions taken by the Subcontractor or Vendor.

4.4 Cooperation. Client shall cooperate with Endeavor IT in investigating and resolving AUP violations, including providing reasonable access to relevant systems, records, and personnel.

4.5 Other Rights and Remedies. Endeavor IT's rights under this AUP are in addition to, and not in lieu of, all other rights and remedies available to Endeavor IT under the Agreement or applicable law, including Endeavor IT's rights under MTC Section 3.4 (Termination for Material Breach) and MTC Section 4.3 (Suspension for Non-Payment).

5. Reporting Violations

5.1 Any person may report a suspected violation of this AUP by emailing abuse@endeavorit.com. To assist Endeavor IT in investigating the report, please include:

(a) a description of the suspected violation;

(b) the affected service, account, or system, to the extent known;

(c) any supporting evidence, including log excerpts, message headers, or screenshots; and

(d) the reporter's contact information.

6. Modifications

6.1 Endeavor IT may modify this AUP from time to time. Modifications are governed by Section 24.5 of the MTC.