ACCEPTABLE USE POLICY

FermTrading, Inc.

Effective Date: September 17, 2026 (revision 2)

THIS ACCEPTABLE USE POLICY GOVERNS YOUR USE OF THE FERM PLATFORM. VIOLATION OF THIS POLICY MAY RESULT IN IMMEDIATE TERMINATION OF YOUR ACCOUNT AND, WHERE THE TERMS AND CONDITIONS OR AN APPLICABLE PROGRAM AGREEMENT AUTHORIZE IT (INCLUDING FRAUD, SANCTIONS, OR OTHER PROHIBITED CONDUCT), DENIAL OR CLAWBACK OF AMOUNTS THAT HAVE NOT SATISFIED ALL PAYOUT CONDITIONS, AND REFERRAL TO LAW ENFORCEMENT WHERE APPLICABLE.

ARTICLE I - SCOPE AND APPLICATION

1.1 This Acceptable Use Policy ("Policy") sets forth the rules and restrictions governing the use of the website, platform, application, and all related services (collectively, the "Platform") operated by FermTrading, Inc., a Delaware C Corporation ("Company," "Ferm," "we," "us," or "our").

1.2 This Policy applies to all users of the Platform, including evaluation participants, funded simulation account holders, visitors, and any person or entity accessing the Platform in any capacity.

1.3 This Policy supplements and is incorporated by reference into the Company's Terms and Conditions (https://tryferm.com/terms). In the event of a conflict between this Policy and the Terms and Conditions, the Terms and Conditions shall control.

1.4 By accessing or using the Platform, you agree to comply with this Policy. If you do not agree, you must immediately cease all use of the Platform.

ARTICLE II - PERMITTED USE

2.1 The Platform is provided solely for the following purposes:

(a) Creating and managing a user account;

(b) Purchasing and participating in simulated trading evaluations;

(c) Trading on funded simulation accounts in accordance with the applicable Funded Trader Agreement;

(d) Submitting payout requests and completing KYC verification;

(e) Accessing account dashboards, performance analytics, and trading history; and

(f) Communicating with the Company through designated support channels.

2.2 All use of the Platform must be lawful, in good faith, and in accordance with this Policy, the Terms and

Conditions, and all applicable laws and regulations.

ARTICLE III - PROHIBITED CONDUCT - PLATFORM INTEGRITY

3.1 You shall not, and shall not attempt to, engage in any of the following:

(a) Unauthorized Access. Accessing or attempting to access any portion of the Platform, systems, servers, databases, or networks that you are not authorized to access, including other users' accounts, administrative panels, or internal APIs;

(b) Reverse Engineering. Decompiling, disassembling, reverse engineering, or otherwise attempting to derive the source code, algorithms, trading engine logic, risk management systems, pricing mechanisms, or fill algorithms of the Platform;

(c) Scraping and Data Harvesting. Using automated tools, bots, crawlers, scrapers, spiders, or any other automated means to access, collect, extract, copy, or index any content, data, or information from the Platform without the Company's prior written consent;

(d) Interference and Disruption. Interfering with, disrupting, degrading, or impairing the operation, performance, or availability of the Platform or any connected systems, including through denial-of-service (DoS/DDoS) attacks, packet flooding, mail bombing, or deliberate overloading;

(e) Vulnerability Exploitation. Exploiting any bug, error, glitch, vulnerability, or unintended behavior in the Platform's software, trading engine, pricing system, or risk management systems for personal gain or to the detriment of the Company or other users;

(f) Circumvention. Bypassing, disabling, or circumventing any security, authentication, access control, rate-limiting, or technical protection measures implemented on the Platform;

(g) Injection and Manipulation. Introducing malicious code, viruses, trojans, worms, ransomware, spyware, keyloggers, or any other harmful software or code into the Platform or any connected systems;

(h) API Abuse. Accessing the Platform through any unauthorized application programming interface (API), protocol, or method not expressly provided by the Company. The Company's Agent API, accessed with API keys issued through the Platform, is an authorized interface when used within its published rate limits and scopes; and

(i) Load Testing. Conducting unauthorized load testing, stress testing, penetration testing, or security scanning of the Platform without the Company's prior written consent.

ARTICLE IV - PROHIBITED CONDUCT - TRADING INTEGRITY

4.1 You shall not, and shall not attempt to, engage in any of the following:

(a) Unauthorized Automation. Using any automated trading system, expert adviser (EA), bot, script, macro, or programmatic access method to execute trades on the Platform, except through the Company's

Agent API using API keys issued to you through the Platform (as governed by Section 6.2 of the Terms and Conditions) or as otherwise explicitly authorized by the Company in writing. All activity conducted through your Agent API keys is attributed to you and remains subject to this Policy and all trading rules;

(b) Account Sharing or Transfer. Sharing, selling, leasing, renting, sublicensing, or otherwise permitting any third party to access or trade on your account;

(c) Multiple Account Abuse. Creating or operating multiple accounts to circumvent trading rules, risk limits, or breach consequences, or to engage in cross-account hedging or collusion;

(d) Identity Fraud. Registering under a false identity, using another person's identity or documents for KYC verification, or providing false, misleading, or altered information to the Company;

(e) Collusion. Coordinating trades, signals, or strategies with other users or third parties for the purpose of exploiting the Platform's risk mechanics, profit-exclusion windows, or evaluation criteria;

(f) Market Manipulation. Engaging in wash trading, simulated trading with no genuine market risk, spoofing, layering, or any other form of market manipulation within the simulated environment;

(g) Latency Exploitation. Exploiting data feed latency, price discrepancies between providers, or execution delays for systematic profit (latency arbitrage, tick sniping); and

(h) Abuse of Platform Features. Deliberately exploiting any feature, rule, or mechanic of the Platform in a manner inconsistent with its intended purpose, as determined by the Company in its reasonable discretion.

ARTICLE V - PROHIBITED CONDUCT - GENERAL

5.1 You shall not use the Platform to:

(a) Violate Laws. Engage in any activity that violates applicable local, state, national, or international laws, regulations, or sanctions, including anti-money laundering (AML), counter-terrorism financing (CTF), and sanctions laws;

(b) Fraud. Engage in fraudulent activity, including initiating unjustified chargebacks, payment fraud, or misrepresentation of eligibility;

(c) Harassment. Harass, threaten, intimidate, stalk, or abuse any Company employee, contractor, or other user;

(d) Defamation. Publish false, misleading, or defamatory statements about the Company, its officers, employees, or services;

(e) Spam. Send unsolicited communications, advertisements, or promotional materials to other users or through Company systems;

(f) Impersonation. Impersonate the Company, its employees, or any other person or entity, or falsely represent an affiliation with the Company;

(g) Intellectual Property Infringement. Infringe upon the Company's intellectual property rights, including trademarks, copyrights, trade secrets, or proprietary information;

(h) Illegal Content. Transmit, upload, or distribute any content that is illegal, obscene, threatening, or that promotes violence, discrimination, or illegal activity; and

(i) Sanctions Evasion. Use VPNs, proxies, remote desktops, relays, false identity information, or any other tools or methods to circumvent geographic restrictions, disguise your true location, or access the Platform from a Restricted Jurisdiction listed in the Terms and Conditions, currently: Afghanistan; Belarus; Cuba; the Democratic Republic of the Congo; Iran; Iraq; Libya; North Korea; Russia; South Sudan; Sudan; Syria; the Central African Republic; Lebanon; Mali; Myanmar; Nicaragua; Somalia; Venezuela; Yemen; Zimbabwe; China; Turkmenistan; Crimea/Sevastopol (Ukraine); Donetsk (Ukraine); Luhansk (Ukraine).

ARTICLE VI - MONITORING AND ENFORCEMENT

6.1 Right to Monitor. The Company reserves the right to monitor Platform usage, trading activity, account behavior, and system access logs to detect violations of this Policy. Monitoring may be automated, manual, or a combination thereof.

6.2 Investigation. The Company may investigate any suspected violation of this Policy. During an investigation, the Company may impose proportionate temporary access restrictions and a documented hold on affected payments where authorized by the applicable agreement or law. Reviews must be pursued without unreasonable delay. A hold is not a forfeiture and does not extinguish approved or accrued payment obligations.

6.3 Enforcement Actions. Upon a reasonable, documented determination of a violation, the Company may take one or more proportionate actions authorized by the applicable agreement or law. Notice and material reasons will be provided unless prohibited by law or inconsistent with a legitimate investigation; the User may request review of a factual or calculation error. Available actions include:

(a) Issue a warning;

(b) Temporarily suspend Platform access;

(c) Permanently terminate all accounts associated with the violating user;

(d) Deny unearned amounts or recover an affected payment only on a documented ground authorized by the applicable agreement or law. Account closure alone does not extinguish approved Payouts, accrued Eligible Net Profits satisfying the applicable conditions, or preserved pre-breach requests;

(e) Seek repayment or lawful set-off of a specifically identified erroneous or fraudulently obtained payment, limited to the affected amount and any further remedy lawfully available;

(f) Report the violation to law enforcement authorities;

(g) Pursue civil remedies, including injunctive relief and damages; and

(h) Share necessary, accurate information with authorized fraud-prevention providers where permitted by applicable privacy law, with available correction and challenge rights.

6.4 No Obligation. The Company is not obligated to monitor for or enforce every violation of this Policy. Failure to enforce any provision shall not constitute a waiver of the Company's right to enforce such provision in the future.

ARTICLE VII - REPORTING VIOLATIONS

7.1 If you become aware of any violation of this Policy, or any security vulnerability, bug, or exploit in the Platform, you are encouraged to report it to:

Email: hello@ferm.trade
Subject: AUP Violation Report (or) Security Vulnerability Report

7.2 Responsible Disclosure. If you discover a security vulnerability, please report it to us before disclosing it publicly. The Company will not take legal action against individuals who discover and report vulnerabilities in good faith, provided they:

(a) Do not exploit the vulnerability beyond what is necessary to confirm its existence;

(b) Do not access, modify, or delete other users' data;

(c) Do not disrupt Platform operations; and

(d) Provide the Company with reasonable time to remediate the issue before public disclosure.

ARTICLE VIII - THIRD-PARTY SERVICES

8.1 The Platform may integrate with or link to third-party services (including but not limited to Persona for KYC, payment processors, and market data providers). Your use of such third-party services is subject to their respective terms of service and acceptable use policies.

8.2 The Company is not responsible for the content, practices, or policies of third-party services. Violations of third-party terms that affect the Platform may be treated as violations of this Policy.

ARTICLE IX - MODIFICATIONS

9.1 The Company reserves the right to modify this Acceptable Use Policy at any time. Changes shall be effective upon posting to the Company's website. The "Effective Date" at the top of this document indicates the date of the most recent revision.

9.2 Continued use of the Platform after modifications constitutes acceptance of the revised Policy.

ARTICLE X - GOVERNING LAW

10.1 This Policy shall be governed by and construed in accordance with the laws of the State of Delaware, United States of America, without regard to its conflict of laws principles.

10.2 Any disputes arising from or related to this Policy shall be resolved in accordance with the dispute resolution provisions of the Company's Terms and Conditions.

ARTICLE XI - CONTACT

For questions regarding this Acceptable Use Policy, please contact:

FermTrading, Inc.
4335 Cadieux Road, Detroit, MI 48224, United States
Email: hello@ferm.trade
Legal: legal@ferm.trade
Website: https://tryferm.com

This Acceptable Use Policy is incorporated by reference into the Company's Terms and Conditions.