TradeRings

LEGAL

TradeRings **Acceptable Use Policy**

VERSION	1.2
EFFECTIVE FROM	17 November 2026
SUPERSEDES	TradeRings Acceptable Use Policy v1.1 (11 June 2026)
OPERATOR	TradeRings Corporation, a Florida corporation (document number P24000001413). Registered address: 55 NE 5th Ave, Suite 501, Boca Raton, FL 33432, USA.

What you should know

1. You may not reverse engineer the Platform or try to work out how it works by any means, including by recording or analysing what goes in and what comes out (section 5.1).
2. You may not use the Platform, its outputs, guides, videos or any data from it to train, fine-tune, distil or prompt any AI model or agent (section 5.7).
3. You may not build, or help anyone build, a product with substantially the same functions as the Platform using what you learned from it, while you use it and for three years after (section 5.8).
4. The Platform's logic, prompts, flows, data models, guides, videos and non-public documentation are TradeRings' confidential information and trade secrets; keep them inside your Account (section 5.9).
5. A breach of section 5 can cost at least USD 1,000,000 for a business account and USD 250,000 for a personal account or an individual, ends every linked Account without notice and bans the people and businesses involved for good (section 9.1).

1. About this Policy

This Acceptable Use Policy (the "AUP") sets out the rules that apply to all use of the TradeRings trading platform, website, mobile applications, integrations, and related services (collectively, the "Platform"). It is the single source of acceptable-use rules across the TradeRings legal framework.

The AUP is incorporated by reference into:

1. The TradeRings Platform Services Agreement (the "PSA"), which binds the Organisation that operates an Account on the Platform.
2. The TradeRings User Terms of Use (the "User Terms"), which binds the individual User at Profile registration.
3. The TradeRings Market Owner Addendum and the Market Member Joining Addendum, which apply to Market-level conduct.

Breach of this AUP is a breach of the agreement under which the breaching party is bound and engages the rights and remedies set out in that agreement, including (without limitation) suspension and termination under PSA clauses 5.5, 6.9, and 10.3.

Defined terms used in this AUP that are not defined here have the meanings given in the PSA.

2. Scope

The AUP applies to:

1. Every individual User in respect of their Profile and their conduct on the Platform (whether or not they are at any time associated with an Organisation).
2. Every Organisation in respect of its Account, its Markets, its Memberships, its Users, and any agent or third party acting on its behalf.
3. Every Market Owner in respect of the operation of its Markets.
4. Every Market Member in respect of its participation in another Organisation's Market.

The Organisation is responsible for ensuring that its Users, agents, and third-party representatives comply with this AUP. Conduct by a User or agent is attributed to the Organisation for the purposes of this AUP.

3. General trading conduct

When engaging in trading activity on the Platform, the Organisation will:

1. Act in good faith in all negotiations and transactions.
2. Provide accurate information about products, pricing, inventory, delivery, and trading terms.
3. Honour commitments made through the Platform, including Confirmed Orders.
4. Not manipulate or attempt to manipulate pricing or market conditions.
5. Not engage in deceptive, fraudulent, anti-competitive, or abusive practices.
6. Comply with all laws and regulations applicable to the trade in every jurisdiction relevant to the Transaction.

4. Prohibited items

The Platform may not be used to list, trade, or facilitate transactions involving:

1. Goods or services prohibited by law or regulation in any jurisdiction relevant to the Transaction.
2. Goods or services subject to international sanctions or export controls, where the Organisation does not hold all licences and authorisations required for the trade.
3. Counterfeit goods, or goods that infringe any third party's intellectual property rights.
4. Stolen goods, or goods of doubtful provenance.
5. Weapons, firearms, ammunition, explosives, military equipment, controlled substances, hazardous materials, human tissue or remains, or live animals, except where the Organisation holds all licences and authorisations required for the trade in every jurisdiction relevant to the Transaction and the Market is specifically configured by the Market Owner for that category.
6. Goods derived from endangered species, or goods sourced from unlawful wildlife trade.
7. Goods, services, or content involving the exploitation, abuse, or endangerment of children.
8. Goods, services, or content promoting terrorism, hate, or violence.

9. Gambling, betting, lotteries, or other gambling-related goods or services, except where the Organisation holds all licences and authorisations required for the trade in every jurisdiction relevant to the Transaction and the Market is specifically configured by the Market Owner for that category.
10. Goods the Organisation does not have the right to sell.

The Market Owner is responsible for ensuring that prohibited items are not listed, traded, or facilitated in its Market, whether by the Market Owner itself or by any Member. The Member is responsible for not listing or transacting in prohibited items as part of its activity in any Market.

TradeRings may remove listings and may suspend or close Accounts or Markets where prohibited items are listed or traded, on the terms set out in clauses 5 and 6 below and in the PSA.

5. Platform integrity

5.1 No reverse engineering

The User and the Organisation will not, and will not assist or permit any other person to, attempt to derive the source code, algorithms, prompts, models, data models, flows, business rules or internal logic of the Platform, including the Automated Order Services (the automated services within the Platform that interpret incoming order signals, match products and customers, apply pricing, validate inventory and order rules, and put orders up for confirmation), by any means. This includes reverse engineering, decompiling and disassembling; observing or systematically recording the Platform's inputs and outputs; probing; screen capture; transcription; and any other analysis intended to reconstruct them. This section applies except to the extent that this restriction is prohibited by applicable law.

5.2 No circumvention

The User and the Organisation will not bypass, disable, or interfere with any security feature, access control, fee mechanism, sanction, suspension, monitoring system, audit trail, or other integrity control of the Platform.

5.3 No platform circumvention to avoid fees

The Organisation will not use the Platform to facilitate trades and then conclude those trades off-Platform with the same counterparties in order to avoid Platform fees.

5.4 No scraping or automated access

The User and the Organisation will not use any robot, spider, scraper, or other automated means to access the Platform other than through documented APIs and integrations, and only then with the prior written permission of TradeRings.

5.5 No impersonation

The User will not create more than one Profile for themselves, will not create a Profile in someone else's name, and will not impersonate any other person on the Platform. The Organisation will not configure its Account to misrepresent the identity, authority, or status of any User, Member, or counterparty.

5.6 Credential security

Each User is responsible for keeping their Profile credentials confidential. Users will not disclose passwords or authentication factors to anyone else, including colleagues at the same Organisation. Each person who needs Platform access must register their own Profile.

5.7 No AI training or distillation

The User and the Organisation will not use, and will not permit anyone acting for them to use, the Platform, its interface, outputs, API responses, documents, guides, videos, support content or any data obtained through the Platform to train, fine-tune, distil, evaluate, benchmark, prompt or ground any machine-learning model, AI system or AI agent, or as or within a dataset for any of those purposes.

5.8 No competing product

During the period in which the User or the Organisation has access to the Platform, and for three years after that access ends (the "restricted period"), the User and the Organisation will not design, build, help to build, fund, advise on or supply a product or service that has substantially the same functions as the Platform, using anything learned from or through the Platform. This section does not apply to independent development that the party proves, from records made at the time, was carried out without access to the Platform or to anything learned from it.

5.9 Confidential information and trade secrets

The following are TradeRings' confidential information and trade secrets, within the meaning of the Defend Trade Secrets Act (18 U.S.C. §1836 and following) and the Florida Uniform Trade Secrets Act: the Platform's order-interpretation logic, prompts, flows, data models and business rules; the guides, documentation, videos and support content served inside the Platform; non-public documentation; and anything marked as confidential or that a reasonable person would understand to be confidential. The sign-in gate, the acceptance record, this AUP and the access controls of the Platform are among the reasonable measures TradeRings takes to keep them secret. The User and the Organisation will not disclose any of them to anyone outside the Account's authorised Users.

5.10 Technological protection measures

Sign-in, access controls, rate limits, export limits, watermarks and session controls on the Platform are technological measures that control access to TradeRings' copyright works (17 U.S.C. §1201) and access controls on its computers (18 U.S.C. §1030). Circumventing, removing or defeating any of them is a breach of this AUP and may also be a statutory wrong.

5.11 Who is bound

This section 5 binds every User, the Organisation, and the Organisation's owners, directors, employees, contractors, agents and affiliates, and applies to any AI tool or AI agent that any of them operates. The Organisation procures their compliance and is liable for their acts as if they were its own. Sections 5.1 and 5.7 to 5.12 continue to apply for five years after the Profile or the Account is closed; section 5.8 applies for the restricted period.

5.12 Presumption

A product or service with substantially the same functions, flows, prompts, outputs or guide content as the Platform that is launched during the restricted period by a User, an Organisation, any of their affiliates, or anyone to whom any of them gave access to the Platform, is presumed to have been derived from the Platform in breach of this section 5, unless the party proves otherwise from records made at the time.

6. Communications

6.1 No abusive conduct

The User will not use the Platform to send, post, or transmit content that is abusive, offensive, threatening, harassing, defamatory, unlawful, or that infringes any third party's rights. The User will not use the Platform to attempt to deceive, defraud, or otherwise harm any other User, Organisation, or third party.

6.2 Monitoring

TradeRings reserves the right to monitor communications conducted through the Platform for compliance with this AUP and the rest of the legal framework.

6.3 Spam and unsolicited communications

The Organisation will not use the Platform to send unsolicited commercial communications to counterparties outside the legitimate course of trade within a Market the Organisation is properly a part of.

7. Data, integrations, and third parties

7.1 Accuracy and lawfulness of data routed through integrations

Where the Organisation connects an ERP system or another Integrated Service to the Platform, the Organisation is responsible for the accuracy and lawfulness of the data it routes through those integrations.

7.2 Third-party rights

The Organisation will respect the intellectual property, privacy, and other rights of third parties when submitting Content, configuring listings, or operating a Market on the Platform.

7.3 No use of the Platform to assist breach of third-party agreements

The Organisation will not use the Platform to assist a counterparty or any other party in breaching an agreement that party has with a third party (for example, breach of an exclusive supply arrangement or of a confidentiality undertaking).

8. Counterparty conduct and identity

The Organisation is solely and exclusively responsible for satisfying itself as to the identity, legitimacy, authority, financial standing, creditworthiness, and reliability of every counterparty with which it interacts on the Platform. The Organisation will not transact on the Platform with any counterparty in circumstances where it knows or reasonably suspects that the counterparty is operating in breach of this AUP, the PSA, or applicable law.

The presence of any Organisation on the Platform is not a representation or warranty by TradeRings as to that Organisation's identity, authority, or fitness to transact. See PSA clauses 3.4, 5.3, and 5.4.

9. Enforcement

9.1 TradeRings' rights

TradeRings may, at its sole discretion and on a reasonable basis:

1. Remove or restrict access to specific Content, listings, or features.
2. Suspend or terminate the access of any User, Account, Market Membership, or Market, in whole or in part, with or without prior notice.
3. Notify affected Market Members of any suspension or termination and of the reason for it, where in TradeRings' judgement that notification is in the interests of those Members or of the Platform.

TradeRings is not required to prove the suspected conduct, to disclose evidence, or to give reasons beyond such description as TradeRings, in its sole discretion, considers appropriate in the circumstances. The full enforcement framework is set out in PSA clauses 5.5, 6.9, 10.3, and 10.4.

A breach of section 5 also carries the remedies in PSA clause 9.4 and User Terms section 8, including liquidated damages, injunctive relief, removal of every linked Account without notice (PSA clause 10.3(5)), forfeiture of originator fees and credits, and a permanent ban on the persons, businesses and devices involved.

9.2 No waiver

The fact that TradeRings does not act on a particular breach does not waive TradeRings' right to act on the same or a different breach in future.

9.3 Reporting breaches

Users and Organisations may report suspected breaches of this AUP to abuse@traderings.io. We treat reports as confidential to the extent practicable and may contact the reporter for further information.

10. Changes to this AUP

TradeRings may update this AUP from time to time. The version and date at the top are revised when we do. Where a change materially expands the obligations on Users or Organisations, we will give notice on the Platform; for Organisations, where the change is material in respect of the PSA, re-acceptance is governed by PSA clause 14, and for individuals by User Terms clause 9.

11. Contact

Questions about this AUP may be directed to legal@traderings.io. Reports of breach may be directed to abuse@traderings.io.