

Prohibited Goods & Services Policy

Version 1.0 · Effective July 18, 2026

1. Purpose

This Prohibited Goods & Services Policy ("Policy") defines the categories of goods, services, and conduct that may not be transacted, referenced, listed, or otherwise facilitated using escrow vaults, milestone trades, or marketplace listings created through the Garantor DAO protocol ("Garantor," "the Protocol"). It exists to protect users, to guide the Garantor DAO's on-chain arbitration decisions, and to set clear expectations for anyone creating or participating in a trade.

2. Scope & Applicability

This Policy applies to every user — buyers, sellers, referrers, stakers, and arbitrators — interacting with any Garantor smart contract deployment, including:

- V1 native-TON regular and milestone escrow vaults
- V2 USDT / jetton-denominated escrow and milestone vaults
- V3 oracle-settled marketplace listings for physical and commodity trades
- Any associated off-chain services, including the Telegram bot, web application, and notification infrastructure

It applies regardless of which network a vault is deployed on (TON Mainnet or Testnet).

3. Nature of the Protocol

Garantor is a non-custodial, decentralized protocol. Smart contracts hold funds in escrow according to on-chain logic; no Garantor DAO member, arbitrator, or affiliated party takes custody of funds outside the protocol's dispute-resolution process. Garantor does not pre-screen trade terms before a vault is deployed and cannot unilaterally reverse a completed on-chain settlement.

This Policy governs acceptable use of the Protocol and informs the DAO's arbitration decisions when a dispute is raised. It does not represent, and should not be read as, custodial control over user funds.

4. Prohibited Categories

The following categories of goods, services, and conduct may not be transacted or facilitated through the Protocol. This list is illustrative, not exhaustive — any trade that is unlawful in the buyer's or seller's jurisdiction is prohibited regardless of whether it appears below.

- 1 **Illegal Drugs & Controlled Substances** — including precursor chemicals, synthetic drugs, and prescription medication sold without valid authorization.

- 2 **Weapons, Ammunition & Explosives** — firearms, firearm parts or conversion devices, ammunition, explosives, and incendiary devices.
- 3 **Counterfeit & Pirated Goods** — counterfeit currency, replica goods misrepresented as genuine, pirated software or media, and any goods infringing a third party's intellectual property.
- 4 **Stolen Property** — goods known or reasonably believed to be stolen, including stolen vehicles, electronics, or financial instruments.
- 5 **Human Exploitation** — human trafficking, forced labor, sexual exploitation, or any service facilitating the exploitation of a person.
- 6 **Child Sexual Abuse Material (CSAM)** — any content depicting or sexualizing minors. Zero tolerance — confirmed instances are reported to the relevant authorities immediately.
- 7 **Non-Consensual Content** — non-consensual intimate imagery (“revenge porn”) or any content obtained or distributed without the subject's consent.
- 8 **Wildlife & Endangered Species** — trade in endangered species or protected wildlife products (e.g., ivory, exotic pelts), or any goods violating CITES.
- 9 **Hazardous Materials** — toxic chemicals, radioactive material, biological agents, or other materials posing a public-health or environmental hazard.
- 10 **Fraudulent Financial Instruments** — counterfeit or altered currency, unauthorized securities, stolen payment-card data, phishing kits, or forged identity documents.
- 11 **Sanctioned Parties & Jurisdictions** — trades involving individuals, entities, or jurisdictions subject to OFAC, UN, EU, or other applicable sanctions regimes.
- 12 **Money Laundering & Structuring** — using escrow vaults to disguise the origin of illicit funds, or structuring transactions to evade reporting thresholds.
- 13 **Unlicensed Financial Services** — unregistered securities offerings, unlicensed money transmission, or unregistered investment schemes conducted through vault terms.
- 14 **Malware & Unauthorized Access Tools** — hacking tools, malware, ransomware, exploit kits, or services offering unauthorized access to systems or accounts.
- 15 **Deceptive Services** — academic-cheating services, fake reviews or engagement, or deepfake-for-hire services intended to deceive a third party.
- 16 **Ponzi & Pyramid Schemes** — any scheme promising returns primarily from recruiting new participants rather than legitimate trade or investment activity.
- 17 **Weapons-Adjacent Digital Goods** — instructions, blueprints, or files for manufacturing weapons or explosives, including 3D-printable firearm components.
- 18 **Any Other Unlawful Goods or Services** — anything unlawful under the law of the buyer's or seller's jurisdiction, or that violates applicable TON Foundation or Telegram platform policies.

5. User Obligations

- Users represent that any trade they create or participate in does not involve a prohibited category listed above.
- Users are solely responsible for confirming the legality of a trade under their own and their counterparty's applicable law.
- Sellers listing goods on the V3 oracle marketplace additionally represent that shipping documentation and delivery data they submit are accurate and have not been falsified.

6. Enforcement

Garantor DAO cannot physically inspect goods or verify off-chain conduct, and does not pre-approve vault terms before deployment. Where a dispute is raised and submitted evidence indicates a trade involves a prohibited category, DAO arbitrators may resolve the dispute against the party responsible for the prohibited listing, consistent with the Protocol's existing on-chain dispute-resolution mechanism.

Repeated or severe violations may result in the offending wallet address being flagged to the community, denial of Commissionaire staking rewards tied to the offending trade, or referral to appropriate law-enforcement authorities. Garantor DAO reserves the right to decline off-chain support (e.g., Telegram bot notifications, marketplace listing indexing) for wallets or listings associated with confirmed violations, to the extent such services are within Garantor's control.

7. Reporting Violations

Suspected violations can be reported via Telegram at @garantor_dao. Reports should include the vault address, a description of the concern, and any supporting evidence.

8. Relationship to Dispute Resolution

This Policy supplements, and does not replace, the Protocol's existing dispute-resolution mechanism. Arbitrators evaluate disputes based on submitted on-chain evidence — document hashes, delivery reports, and transaction records — and this Policy provides the standard against which listing legitimacy is judged.

9. Policy Updates

This Policy may be updated from time to time as the Protocol evolves — for example, as new vault types are introduced or new jurisdictions are served. The current version is always available on garantor.io and via the in-app Help & Guide panel. Material changes will be announced through the Garantor DAO Telegram channel.

10. Contact

Telegram: @garantor_dao

Web: garantor.io

