TRD NETWORK

LEGAL · EFFECTIVE JUNE 2026

# Acceptable Use Policy

## TRD Network

This Policy defines workloads and conduct that are not permitted on TRD Network. It protects the network, its providers, and other users, and is incorporated into the Terms of Service.

## 1. Purpose

This Acceptable Use Policy ("AUP") sets the rules for using TRD Network. It applies to all renters, providers, and agents operating on the network. Violations may result in suspension or termination and, where appropriate, referral to authorities.

This Acceptable Use Policy ("AUP") sets the rules for using TRD Network. It applies to all renters, providers, and agents operating on the network. Violations may result in suspension or termination and, where appropriate, referral to authorities.

## 2. Prohibited content & workloads

- Anything unlawful, or that infringes intellectual-property or privacy rights.
- Material that sexually exploits or endangers minors (zero tolerance; reported as required by law).
- Malware, ransomware, exploit development, or tooling whose primary purpose is to compromise systems.
- Workloads designed to enable weapons of mass destruction or other serious physical harm.
- Content that incites violence or targeted harassment.

## 3. Prohibited conduct

- Attempting to access, inspect, or interfere with another tenant's workloads or data.
- Circumventing metering, billing, rate limits, or security controls.
- Disrupting the network, providers, or dispatch (e.g. DoS, resource exhaustion attacks).
- Reverse-engineering provider isolation or extracting other users' keys or secrets.
- Misrepresenting hardware as a provider, or manipulating benchmarks or reputation.

## 4. High-risk & regulated sectors

For sensitive sectors — health, defence, government and finance — TRD's role is provenance and audit (a research and audit layer), not domain decision logic. Do not deploy the Service as an autonomous decision-maker in safety- or rights-critical contexts without appropriate human oversight and your own compliance controls.

## 5. Security research

Good-faith security testing of your own workloads is permitted. Testing that targets the network, other tenants, or providers without authorization is prohibited. Report vulnerabilities to security@trdn.io.

## 6. Provider responsibilities

Providers must run only the authorized worker software, must not tamper with tenant workloads, and must maintain hardware they are entitled to operate. Providers are responsible for the legality of operating their hardware in their jurisdiction.

## 7. Enforcement

We may investigate suspected violations, remove or suspend offending workloads, throttle or terminate accounts, and preserve and disclose information where legally required or necessary to protect the network and its users.

## 8. Reporting

Report abuse, prohibited content, or security issues to abuse@trdn.io or security@trdn.io. We review reports and act proportionately.

## 9. Changes

We may update this AUP as the network and threat landscape evolve; the current version governs your use.