

Fors33 Acceptable Use Policy

Last Updated: March 29, 2026

1. Purpose and Scope: This Acceptable Use Policy establishes strict operational boundaries for utilizing Fors33 software, APIs, and services. It is designed to protect our infrastructure and ensure deterministic performance for all operators. By accessing our systems, you agree to comply with this policy in its entirety.

2. Absolute Prohibitions: You are strictly forbidden from using Fors33 products to engage in, promote, or facilitate any of the following activities:

- **Illegal Acts:** Any violation of applicable local, state, national, or international law.
- **Malicious Operations:** Distributing malware, executing ransomware, or intentionally compromising third-party systems.
- **Cryptographic Circumvention:** Attempting to forge, alter, or bypass the cryptographic proofs, sidecars, or validation mechanisms generated by our tools.
- **Reverse Engineering:** Decompiling, disassembling, or attempting to extract the underlying source code or proprietary logic of any Fors33 application.

3. Infrastructure Integrity: Our APIs and verification systems must remain highly available. You do not have permission to:

- Execute denial-of-service attacks or intentionally overload our endpoints.
- Probe, scan, or test the vulnerability of our networks without explicit written authorization.
- Attempt to access internal administrative interfaces or data belonging to other tenants.
- Interfere with the proper functioning of any software deployed on our servers.

4. Credential and License Abuse: Your access is tied to your specific operator identity. You must not:

- Share, resell, or distribute your license keys to unauthorized third parties.

- Automate the creation of accounts or exploit free tiers to bypass paid seat requirements.
- Obscure your operational origin using unauthorized proxy networks to evade rate limits or geographic restrictions.

5. Enforcement and Authority: Fors33 retains absolute authority to enforce this policy. We monitor API telemetry and cryptographic validation requests to detect abuse. If we determine that you have violated any provision of this Acceptable Use Policy, we will take immediate action. This includes the immediate suspension or permanent termination of your account, revocation of all active license keys, and forfeiture of any prepaid subscription fees. We reserve the right to report severe violations to the appropriate legal authorities without prior notice.

6. Export Compliance and Sanctions: Fors33 software and services are subject to the export control and economic sanctions laws of the United States. By utilizing the Services, you represent and warrant that you are not located in, under the control of, or a national or resident of any embargoed country or territory. You further warrant that you are not listed on any U.S. Government list of prohibited or restricted parties. You agree not to export, re-export, or transfer the Services in violation of these laws.

7. Content and Data Legality: While Fors33 operates locally and does not host your raw datasets, you are strictly prohibited from using our Services to cryptographically seal, verify, or facilitate the transfer of data that is illegal, promotes violence, infringes on third-party intellectual property rights, or contains child sexual abuse material (CSAM).

8. Fair Usage and API Limits: To ensure deterministic performance and stability across all Lab and Pro tenants, our APIs are subject to fair use thresholds and automated rate limiting. Fors33 reserves the absolute right to throttle, cap, or temporarily suspend your API access if your request volume significantly exceeds standard operational parameters or threatens overall system integrity.

9. Abuse Reporting: Fors33 investigates all credible reports of policy violations. If you believe a user or tenant is violating this Acceptable Use Policy, you must report the activity immediately to: reportabuse@fors33.com.