

Acceptable Use Policy

Rules for Responsible Use of Jollybyte Studios™ Services, Including Womdock™

Effective Date August 30, 2026

Company Website www.Jollybyte-Studios.com

Womdock™ Website www.womdock.com

Legal Contact info@jollybyte.co

This Acceptable Use Policy (“AUP”) establishes rules for use of Jollybyte Studios™ websites, Womdock™, software, applications, downloads, network resources, and services. It is designed to protect users, third parties, Jollybyte Studios™, and the security and reliability of our systems.

Womdock™ is a product of Jollybyte Studios™. This revision expressly includes Womdock™, www.womdock.com, and applicable Womdock™ software and services within this policy where stated.

Contents

Scope • Unlawful Use • Security Abuse • Malware • Service Disruption • Automated Access • Fraud and Deception • Harassment • Dangerous Misuse • Intellectual Property • Privacy • Third-Party Providers • Credential Abuse • Enforcement Evasion • Reporting • Enforcement • Changes • Contact

1. Scope and Responsibility

This AUP applies whenever you access or use a Jollybyte Studios™ Service, including Womdock™, or use a Jollybyte Studios™ Service as part of a workflow involving third-party systems. You are responsible for your conduct, content, credentials, configurations, automation, and use of outputs.

2. Unlawful or Rights-Violating Use

You may not use the Services to commit, facilitate, promote, instruct, or conceal unlawful activity; infringe or misappropriate copyright, trademark, trade secret, privacy, publicity, contractual, or other rights; unlawfully obtain, disclose, sell, or distribute personal or confidential information; or evade lawful restrictions, sanctions, court orders, or regulatory obligations. You are responsible for obtaining necessary rights and permissions for content you import, process, generate, modify, publish, or distribute.

3. Security Abuse and Unauthorized Access

You may not probe, scan, exploit, or test vulnerabilities of Jollybyte Studios™ systems, Cloudflare configurations, networks, accounts, software, licensing mechanisms, or infrastructure without explicit written authorization. You may not gain or attempt to gain unauthorized access; bypass authentication or authorization; defeat rate limits or technical restrictions; intercept traffic without authorization; introduce backdoors; exploit vulnerabilities; or interfere with security logging, integrity checks, or anti-abuse controls.

4. Malware and Harmful Code

You may not use the Services to create, deliver, host, distribute, or facilitate malware, ransomware, destructive payloads, credential stealers, botnets, malicious scripts, exploit kits, or code intended to damage, disrupt, surveil, or gain unauthorized control of systems. Legitimate defensive security research or educational material must be conducted lawfully, within authorized environments, and without targeting systems or data you do not have permission to test.

5. Service Disruption and Resource Abuse

You may not intentionally degrade, overload, flood, deny service to, disrupt, or materially impair the Services or related infrastructure. You may not consume excessive resources in a manner designed to evade reasonable limits or disrupt other users. You may not manipulate traffic, requests, or workflows to bypass protective controls or create disproportionate load.

6. Automated Access, Scraping, Bots, and Crawlers

You may not launch or operate robots, spiders, scrapers, offline readers, headless clients, automated request systems, or other automated means against www.jollybyte-studios.com, www.womdock.com, or Jollybyte Studios™ infrastructure in a manner that exceeds reasonable human use, violates technical directives, bypasses access restrictions, degrades service, or collects data without authorization.

7. Spam, Fraud, Deception, and Coordinated Inauthentic Behavior

You may not use the Services to send or facilitate unsolicited bulk communications in violation of law; operate scams, phishing, credential theft, fraudulent transactions, or deceptive schemes; impersonate another person or organization in a manner intended to deceive or cause harm; or coordinate fake accounts, fabricated engagement, or inauthentic behavior designed to mislead platforms, customers, voters, advertisers, or the public. You may not misrepresent the source, sponsorship, endorsement, authenticity, or provenance of content when doing so would be unlawful or materially deceptive.

8. Harassment, Threats, and Exploitation

You may not use the Services to facilitate credible threats, stalking, targeted harassment, doxxing, extortion, exploitation, trafficking, or abuse. You may not create or distribute sexual content involving minors, child sexual abuse material, grooming material, or sexual exploitation of children under any circumstances. You may not create or distribute non-consensual intimate imagery, sexualized material depicting an identifiable person without required consent, or content intended to facilitate sexual exploitation or blackmail.

9. Dangerous and Highly Regulated Misuse

You may not use the Services to facilitate unlawful acquisition, manufacture, trafficking, or deployment of weapons, explosives, controlled substances, or other regulated goods, or to provide operational assistance for violent criminal activity.

Lawful professional, educational, documentary, compliance, or safety-related content may be permitted when used responsibly and within applicable law.

10. Intellectual Property Abuse

You may not remove or falsify copyright, trademark, attribution, licensing, watermark, provenance, or rights-management information in order to misrepresent ownership or facilitate infringement. You may not use Jollybyte Studios™ intellectual property, branding, software, code, documentation, or assets beyond the rights granted by applicable license terms.

11. Privacy and Personal Data

You may not use the Services to unlawfully collect, infer, expose, trade, or misuse personal information; circumvent privacy settings; obtain credentials; or create databases of sensitive personal information without lawful authority and appropriate safeguards. If your workflow processes personal information, you are responsible for determining your legal obligations, including notice, consent, retention, security, and data-subject rights where applicable.

12. Third-Party Providers and Connected Services

When Womdock™ or another Jollybyte Studios™ Service connects to a third-party provider or service at your direction, you must comply with that provider's rules, rate limits, content policies, licensing restrictions, and account terms.

13. Credential and API Abuse

You may not use credentials, API keys, access tokens, accounts, licenses, or payment methods without authorization. You may not sell, share, harvest, or traffic in compromised credentials or use Jollybyte Studios™ software to conceal unauthorized use of a provider account. You are responsible for protecting credentials you configure and for rotating or revoking them if compromised.

14. Attempts to Evade Enforcement

You may not evade or attempt to evade account restrictions, IP blocks, security challenges, rate limits, license controls, abuse-detection systems, or other enforcement measures through alternate accounts, proxies, credential rotation, spoofing, automation, or similar techniques.

15. Reporting Security Issues and Abuse

If you identify a security vulnerability or suspected abuse involving Jollybyte Studios™ infrastructure, contact info@jollybyte.co with sufficient information for us to investigate. Do not publicly expose sensitive details, access data that is not yours, or continue testing beyond what is necessary to demonstrate the issue without authorization. Copyright complaints should follow the DMCA & Copyright Policy. Technical-support issues should be directed to the support address listed below.

16. Enforcement

Jollybyte Studios™ may investigate suspected violations and may warn, rate-limit, block, suspend, restrict, terminate, or refuse access; remove or disable content we control where appropriate; preserve relevant records; cooperate with providers or lawful authorities; and pursue legal remedies. Enforcement decisions may consider severity, intent, history, risk, legal obligations, technical feasibility, and whether the issue can reasonably be cured. We are not obligated to provide advance notice where immediate action is necessary to protect security, prevent harm, preserve evidence, or comply with law.

17. Changes to This AUP

We may update this AUP as threats, Services, infrastructure, or legal requirements evolve. The current version will be posted through www.Jollybyte-Studios.com with an updated effective or revision date.

18. Contact

Legal, security, or abuse reports: info@jollybyte.co.

Technical support: support@jollybyte.co.

Company website: www.Jollybyte-Studios.com.

Womdock™ website: www.womdock.com.

Document Control

Policy owner: Jollybyte Studios™. Effective date: August 30, 2026. The versions posted on www.Jollybyte-Studios.com and, where applicable, www.womdock.com are intended to be the current public versions.