

[Home](#) / [Governance](#) / [Acceptable Use Policy](#)

Acceptable Use Policy (AUP)

Effective Date: August 28, 2026 • **Applies to:** All Hosted Groups, Subdomains & Infrastructure

Version 1.0

Why This Policy Protects the Entire Community

Sky Waters operates on shared, community-subsidized OpenBSD infrastructure. A single compromised script, spam campaign, or abusive workload puts the IP reputation, server uptime, and security of **every grassroots partner group** at risk with our upstream providers. Violations will result in immediate suspension without warning.

1. Purpose & Scope

This Acceptable Use Policy ("AUP") outlines the rules governing the use of all systems, networks, servers, databases, subdomains (e.g., *.skywaters.org), storage volumes, and web services provided by **Sky Waters** ("Sky Waters," "we," "us").

This policy applies to all organizations, organizers, volunteers, and visitors who access or utilize Sky Waters resources. Compliance with this AUP is a mandatory condition of receiving donated hosting, technical support, or subdomain allocation.

2. Strictly Prohibited Activities & Content

You agree not to use Sky Waters infrastructure, networks, or subdomains to host, transmit, store, or link to any of the following:

A. Malicious Code, Attacks & Network Exploits

Malware, ransomware, Trojan horses, rootkits, botnet command-and-control (C2), keyloggers, or spyware.

Phishing sites, fraudulent donation scams, credential harvest forms, or deceptive impersonation of individuals, financial institutions, or other non-profit entities.

Network abuse, including unauthorized port scanning, vulnerability fuzzing, denial-of-service (DoS/DDoS) attacks, relay exploitation, or packet spoofing.

B. Spam & Bulk Unsolicited Communications

Sending unsolicited bulk email (spam), commercial advertising, chain letters, or unsolicited text/SMS messages.

Operating open mail relays or unauthenticated webmail forms that allow third parties to emit spam.

Harvesting or scraping email addresses or personal phone numbers without affirmative consent.

Mailing List Requirement: Any automated newsletters or community mailing lists (e.g., Listmonk) must be 100% permission-based opt-in with a working, one-click unsubscribe mechanism, and must route through an authorized external transactional relay.

C. Unlawful & High-Harm Content

Child Sexual Abuse Material (CSAM) or Child Sexual Exploitation and Abuse (CSAE). Any occurrence will result in immediate termination, server wiping, and mandatory reporting to the National Center for Missing & Exploited Children (NCMEC) and law enforcement.

Non-consensual sexual imagery, revenge pornography, or intimate deepfakes.

Incitement of imminent physical violence, targeted death threats, or terroristic communications.

Doxxing or the non-consensual publication of personal residential addresses, personal phone numbers, or private confidential details intended to endanger or harass individuals.

D. Resource Mining & Network Degradation

Cryptocurrency mining (e.g., Monero, Bitcoin, or any proof-of-work algorithm) under any circumstances.

High-bandwidth video restreaming, file warehousing, BitTorrent trackers, or seedboxes.

Running automated scraping bots, web crawlers, or high-concurrency stress tests against external targets.

3. Prohibited Regulated Data (High-Risk Categories)

Because Sky Waters operates as a volunteer initiative on a lean budget, **our infrastructure is NOT certified for regulated, high-liability data categories**. You agree never to store, process, or transmit:

Protected Health Information (PHI): Sky Waters is not a HIPAA Covered Entity or Business Associate. Medical records, patient therapy notes, or clinical intake files may not be hosted on our MariaDB tables or file systems.

Payment Card Industry (PCI-DSS) Data: Never store raw credit card numbers, CVV codes, or bank account routing numbers. Partner groups must utilize established, dedicated payment processors (such as Stripe, Open Collective, or GiveButter) directly.

Government-Issued Identification Numbers: Social Security Numbers (SSNs), passport numbers, or driver's license scans.

4. Resource Quotas & Fair Use

To ensure equitable performance across all participating mutual aid groups:

Database Storage: MariaDB instances are intended for relational tables, intake forms, supply lists, and rosters. Large binary objects (BLOBs, video files, raw photo dumps) should not be stored directly within database tables.

Disk Space Caps: Dedicated cloud storage or CryptPad instances carry an initial fair-use cap of **5 GB per organization** unless a higher quota is explicitly approved in writing by Sky Waters maintainers.

Excessive CPU / Memory Load: Workloads that consistently consume over 50% of available CPU or memory resources on the shared OpenBSD host will be throttled or optimized with the partner group.

5. Immediate Unilateral Suspension & Enforcement

5.1 Right to Terminate: Sky Waters reserves the absolute, unilateral right to suspend, rate-limit, disable, or terminate any subdomain, hosted portal, or database account immediately and without prior notice if:

- We suspect or detect a violation of this Acceptable Use Policy;
- A hosted web script or database is compromised by external attackers or emitting spam;
- An upstream provider (Cloudflare, VPS hosting facility) issues an abuse notification or threat of IP termination; or
- Required by court order, valid subpoena, or law enforcement agency.

5.2 Zero Liability for Suspension: Sky Waters and its volunteer maintainers bear zero liability for any downtime, loss of communication, or organizational disruption resulting from enforcement actions taken under this policy.

6. Reporting Abuse & Contact

If you discover a website, subdomain, or service hosted on the Sky Waters network that violates this Acceptable Use Policy, please report it immediately with relevant URLs, logs, and evidence:

Abuse Email: abuse@skywaters.org (cc: hello@skywaters.org)

Response Time: Our volunteer infrastructure team reviews abuse reports within 24–48 hours.