Acceptable Use Policy (AUP) - Sahara Compute LLC

1. Introduction

This Acceptable Use Policy ("AUP") governs the use of services provided by Sahara Compute LLC ("Company"). By using our cloud and VPS platform ("Services"), you agree to comply with this AUP. Violations may result in suspension or termination of services without refund.

2. Prohibited Activities

You may not use Sahara Compute LLC's Services to engage in, foster, or promote illegal, abusive, or harmful activities, including but not limited to:

2.1 Illegal or Unlawful Use

- Hosting, storing, or distributing any content that violates local, state, national, or international laws.
- Engaging in or promoting illegal activities, including fraud, money laundering, and identity theft.

2.2 Malicious or Harmful Activity

- Launching, facilitating, or participating in Distributed Denial-of-Service (DDoS) attacks.
- Spreading malware, ransomware, trojans, viruses, or other malicious software.
- Engaging in hacking, unauthorized access, or exploiting security vulnerabilities.

2.3 Network and System Abuse

- Port scanning, penetration testing, or security scanning without explicit written permission.
- Overloading or attempting to disrupt network stability or system performance.
- Running public resolvers, open mail relays, or open proxies that can be exploited for malicious purposes.

2.4 Spam and Unsolicited Communications

- Sending, facilitating, or hosting bulk unsolicited emails (spam) or participating in mass-marketing schemes.

- Using the services for phishing, deceptive practices, or fraudulent communications.

2.5 Intellectual Property Violations

- Hosting, distributing, or transmitting copyrighted material without proper authorization.
- Engaging in trademark infringement, software piracy, or unauthorized file sharing (e.g., torrents, warez sites).

2.6 Abusive Content

- Hosting or distributing child exploitation materials, including CSAM (Child Sexual Abuse Material).
- Hosting or promoting content that incites violence, hate speech, or discrimination.
- Hosting, promoting, or participating in extremist, terrorist, or illegal activities.

2.7 Resource Abuse

- Excessive resource usage that negatively impacts other customers.
- Mining cryptocurrency without explicit permission from Sahara Compute LLC.
- Running applications that generate excessive I/O, CPU, or network congestion without proper resource allocation.

3. Security and Compliance

- Customers must maintain security best practices, including keeping software and services updated.
- Customers are responsible for securing their accounts, passwords, and API keys.
- Sahara Compute LLC reserves the right to audit and investigate suspected policy violations.

4. Enforcement and Consequences

Violations of this AUP may result in:

- Immediate suspension or termination of services.
- Reporting to law enforcement authorities if applicable.
- Legal action if damages result from prohibited activities.

Sahara Compute LLC reserves the right to modify this policy at any time. Customers are responsible for staying informed of any updates.

5. Reporting Violations

To report violations of this AUP, contact us at support@saharacompute.com.

By using our services, you agree to abide by this AUP. Failure to comply may result in account suspension or termination without refund.