Servernah
By Atlancis

# SERVERNAH CLOUD ACCEPTABLE USE POLICY

*Atlancis Technologies Limited Version 1.0 | Effective Date: 24 February 2026*

| | |
|---|---|
| Document Ref | SNH-AUP-001 |
| Version | 1.0 |
| Effective Date | 24 February 2026 |
| Owner | Head of Business Operations — Atlancis Technologies Limited |
| Review Cycle | Annually or upon material platform change |
| Governing Law | Laws of Kenya |

## 1. Introduction and Purpose

This Acceptable Use Policy (AUP) governs the use of Servernah Cloud services, products, and infrastructure (Services) provided by Atlancis Technologies Limited (Atlancis, we, us) to customers, users, and any third parties accessing the platform (Customer, you).

By accessing or using any Servernah Service, including through the Self-Service Portal (SSP), API, or under an enterprise contract, you agree to be bound by this AUP. This policy exists alongside and is incorporated into the Servernah Terms of Service and any applicable Master Service Agreement (MSA). In the event of conflict, the MSA shall prevail for enterprise customers.

The purpose of this AUP is to protect the integrity, availability, and security of Servernah's infrastructure, to ensure compliance with applicable Kenyan and international law, and to maintain a fair and reliable environment for all Customers.

## 2. Scope

This AUP applies to:

- All Servernah cloud services, IaaS, DBaaS, LBaaS, BaaS, and any future services
- All prepaid (self-service) and enterprise (contract) customers
- All users, employees, contractors, and agents acting on behalf of a Customer
- Any workloads, applications, data, or content hosted on or transmitted through Servernah infrastructure
- All interactions with the Servernah Self-Service Portal (SSP), APIs, support systems, and billing platform

## 3. Permitted Use

Servernah Services are provided for lawful, legitimate commercial and technical purposes. Permitted uses include, but are not limited to:

- Hosting business applications, websites, and enterprise workloads
- Development, testing, and staging environments
- Data storage, backup, and disaster recovery operations
- Running database workloads via the DBaaS platform
- Load balancing production services via the LBaaS platform
- Backup and data protection via the BaaS platform
- Research and development activities that comply with applicable law
- Any other lawful purpose consistent with these terms

## 4. Prohibited Uses

The following activities are strictly prohibited on Servernah infrastructure. Violation of any prohibition in this section may result in immediate suspension or termination of services without notice, and may be reported to relevant law enforcement or regulatory authorities.

### 4.1 Illegal Activities

- Any activity that violates Kenyan law, including the Computer Misuse and Cybercrimes Act 2018, the Kenya Information and Communications Act, the Data Protection Act 2019, or any other applicable legislation
- Hosting, storing, distributing, or transmitting any content that is unlawful, defamatory, obscene, or constitutes child sexual abuse material (CSAM)
- Using the Services to facilitate money laundering, fraud, or other financial crimes
- Any activity that violates applicable export control laws or sanctions regimes

### 4.2 Security Violations

- Attempting to gain unauthorised access to any system, network, or data; whether on Servernah infrastructure or any third party's systems
- Conducting port scans, vulnerability scans, or penetration testing on infrastructure you do not own or have explicit written permission to test
- Deploying malware, ransomware, spyware, viruses, trojans, or any other malicious code
- Intercepting, monitoring, or harvesting data or communications without authorisation
- Circumventing or attempting to circumvent any security measures, authentication controls, or access restrictions on the platform
- Using Servernah infrastructure to conduct attacks against third-party systems, including denial-of-service (DoS or DDoS) attacks, brute-force attacks, or credential stuffing

### 4.3 Network Abuse

- Sending unsolicited bulk email (spam) or operating open mail relays
- Generating traffic volumes that unreasonably degrade the performance of Servernah's shared infrastructure or affect other Customers
- Spoofing IP addresses or otherwise misrepresenting the origin of network traffic
- Operating botnet command-and-control infrastructure
- Engaging in any activity that causes Servernah's IP address ranges to be blocklisted by major ISPs, DNS providers, or anti-spam services

### 4.4 Resource Misuse

- Mining cryptocurrency on Servernah infrastructure without prior written authorisation from Atlancis
- Using Services in a manner inconsistent with the selected service tier or flavour — including attempting to exceed allocated quotas through technical means
- Reselling or sublicensing Servernah Services to third parties without Atlancis's prior written consent
- Using Servernah infrastructure as a proxy or relay to obscure the true origin of harmful traffic

### 4.5 Data and Privacy Violations

- Processing personal data in violation of the Kenya Data Protection Act 2019 or any applicable data protection regulation
- Storing or transmitting sensitive personal data (including health records, financial data, or government identification data) without appropriate security controls and, where required, a Data Processing Agreement with Atlancis
- Transferring personal data outside Kenya in breach of applicable data residency obligations or without appropriate legal basis and customer consent
- Using the platform to conduct unlawful surveillance, stalking, or harassment of individuals

### 4.6 Intellectual Property

- Hosting or distributing content that infringes the copyright, trademark, or other intellectual property rights of any third party
- Using Servernah's trademarks, brand assets, or service names without prior written authorisation

## 5. Responsible Disclosure and Security Research

Atlancis supports responsible security research. If you believe you have discovered a vulnerability in Servernah infrastructure, please disclose it responsibly by contacting ***security@servernah.com*** before any public disclosure. Do not exploit the vulnerability or access data beyond what is minimally necessary to demonstrate its existence.

Authorised security testing of your own Servernah resources is permitted provided you notify Atlancis in advance at ***cloud@servernah.com*** and confine all testing strictly to your own tenancy.

## 6. Customer Responsibilities

Customers are responsible for:

- Ensuring all users, employees, contractors, and agents operating under their account comply with this AUP
- Maintaining the security of account credentials, API keys, and access tokens
- Promptly notifying Atlancis of any suspected security incident, data breach, or compromise of their Servernah account at cloud@servernah.com
- Ensuring any third-party applications or software deployed on Servernah infrastructure comply with applicable law and this AUP
- Maintaining appropriate data protection measures for any personal data processed on the platform

## 7. Monitoring and Enforcement

Atlancis reserves the right to monitor network traffic, resource usage, and platform activity for the purposes of detecting AUP violations, ensuring platform stability, and maintaining security. Atlancis will handle any data collected in accordance with its Privacy Policy.

Upon detecting or receiving credible notice of a potential AUP violation, Atlancis may, at its sole discretion and without prior notice where circumstances require:

- Issue a formal warning to the Customer
- Suspend or throttle the relevant services or workloads
- Terminate the Customer's account and all associated services
- Remove or disable access to offending content or resources
- Report the matter to relevant law enforcement or regulatory authorities
- Pursue any other remedies available under the MSA or applicable law

Where circumstances permit, Atlancis will provide reasonable notice before taking enforcement action. However, in cases involving imminent harm to Servernah infrastructure, other Customers, or third parties, Atlancis may act immediately.

## 8. Reporting Violations

| | |
|---|---|
| **SECURITY ISSUES** | *security@servernah.com* |
| **ABUSE / AUP VIOLATIONS** | *cloud@servernah.com* |
| **GENERAL SUPPORT** | MySupport portal at *portal.servernah.com* |

## 9. Amendments

Atlancis reserves the right to update this AUP at any time. Customers will be notified of material changes via email and through a notice on the Servernah portal. Continued use of the Services after the effective date of any update constitutes acceptance of the revised AUP.

## 10. Governing Law

This AUP is governed by the laws of Kenya. Any dispute arising in connection with this AUP shall be resolved in accordance with the dispute resolution provisions of the applicable MSA or, for prepaid customers without an MSA, in the courts of Kenya.