

ACCEPTABLE USE POLICY (AUP)

Acceptable Use Policy

Provider: Skydexs Hosting

Contact Email: contact@skydexs.com

Effective Date: July 22, 2026

1. Introduction and Scope

This Acceptable Use Policy ("AUP" or the "Policy") governs the use of the virtual web hosting infrastructure and services provided by **Skydexs Hosting** (the "Service").

By using the Service, the Customer fully and unconditionally agrees to comply with this Policy. Compliance with these terms is mandatory for all Customers hosting their websites within the Skydexs Hosting infrastructure.

2. Account Responsibility and Security

Authentication Credentials:

The Customer is solely responsible for safeguarding passwords, access keys, database passwords, and hosting control panel credentials. Any actions performed using the Customer's account shall be deemed to have been performed by the Customer.

Web Application Security:

The Customer is responsible for keeping all content management systems (CMS), plugins, themes, and scripts up to date to prevent unauthorized access by third parties.

Backups:

The Customer is solely responsible for creating and maintaining backups of their website files, databases, and email accounts.

3. Prohibited Content and Activities

The following content and activities are strictly prohibited on Skydexs Hosting servers and network:

3.1 Illegal Content and Activities

- Any content that violates applicable laws or regulations.
- Promotion or distribution of illegal drugs, unlicensed pharmaceuticals, weapons, or forged documents.
- Operation or promotion of unlicensed gambling services, financial pyramid schemes, or fraudulent projects.
- Content promoting violence, extremism, hatred, or national or religious intolerance.
- Any content involving the sexual exploitation of minors.

3.2 Malware and Network Abuse

- Creating or hosting phishing websites, fake login pages, or fraudulent payment systems.
- Hosting or distributing exploits, viruses, malware, network scanners, Trojan software, or malicious scripts.
- Using the hosting service to conduct network attacks, brute-force attacks, vulnerability scanning, or other unauthorized security testing against external systems.

3.3 Spam and Unsolicited Communications

- Sending unsolicited commercial email (spam) of any volume through the hosting mail services or web scripts.
- Using mailing lists or databases collected without the explicit consent of recipients.

3.4 Intellectual Property Protection

- Hosting pirated software, copyrighted media, or publishing links to such resources, including warez websites, torrent trackers, cracked CMS platforms, or unauthorized plugins.
- Using third-party trademarks, logos, or other intellectual property without the permission of the rightful owner.

4. Technical Limitations and Intended Use

Virtual web hosting is intended exclusively for operating websites and related web services. To ensure stable service for all Customers, the following restrictions apply:

- **File Storage:** The Service may not be used as a personal file storage system, backup repository for unrelated systems, download archive for audio or video collections, or as a public file-sharing service.
- **Server and Database Load:** Running continuously operating background processes, autoclickers, cryptocurrency miners, parsers, crawlers, or other software that places excessive or continuous load on CPU, memory, or database servers is prohibited.
- **Traffic Relay:** Operating anonymizers, proxy services, proxy scripts, VPN gateways, or any tools intended to relay or redirect network traffic through the hosting service is prohibited.

5. Infrastructure Protection and Service Availability

Skydexs Hosting implements technical measures to filter malicious traffic and protect hosted websites from Layer 3 and Layer 4 (L3–L4) DDoS attacks.

If an attack of abnormal intensity threatens the stability of infrastructure or other customers' services, Skydexs Hosting reserves the right to temporarily restrict access to the affected domain or IP address.

Temporary website unavailability resulting from protective measures during a DDoS attack shall not be considered a breach of the hosting service agreement.

6. Abuse Reports and Enforcement

All abuse reports, copyright complaints, and legal requests should be sent to:

contact@skydexs.com

If a violation of this Policy is identified, Skydexs Hosting reserves the right, depending on the severity of the violation, to:

- Issue a warning requiring the Customer to resolve the violation within a specified timeframe;
- Temporarily suspend an individual website or domain;
- Permanently suspend the Customer's account without prior notice and without refund in cases of serious violations, including phishing, spam, malware distribution, or DDoS attacks.

7. Final Provisions

Skydexs Hosting reserves the right to amend this Acceptable Use Policy at any time.

Any updated version becomes effective immediately upon publication on the official website.

Continued use of the hosting services after such changes take effect constitutes the Customer's acceptance of the revised Policy.