

Acceptable Use Policy (AUP)

Version: AUP-2026.1

Effective Date: 10.02.2026

Issued by: Hub Hosting

Applies to: All Clients of Hub Hosting

Contact: legal@hub-hosting.com

Jurisdiction: Ireland / European Union

1. Scope and Purpose

This Acceptable Use Policy (AUP) defines acceptable and prohibited uses of services provided by **Hub Hosting**, a commercial brand owned and operated by the company Digital Synergy Ltd, registered in Ireland.

This AUP applies to all clients and all services offered, including but not limited to:

- Fully managed web hosting
- Fully managed virtual private servers (VPS)
- Fully managed cloud storage
- Commercial domain name registration

This policy ensures compliance with:

- General Data Protection Regulation (GDPR) - EU 2016/679
- NIS2 Directive - EU 2022/2555
- eCommerce Directive - EU 2000/31/EC
- ISO/IEC 27001:2022 and SOC 2 Type II - aligned controls

2. Acceptable Use

Clients are required to use Hub Hosting services lawfully, responsibly, and ethically. Acceptable use includes:

- Hosting of legally compliant websites, email services, and databases
- Operating business applications and APIs within defined resource limits
- Storing and processing non-sensitive or CUI (Controlled Unclassified Information) content, if permitted
- Registering and managing domains for legitimate purposes

3. Prohibited Activities

Clients may not use Hub Hosting services for any of the following:

- Sending unsolicited emails, spam, or mass marketing without consent
- Hosting or distributing malware, spyware, ransomware, or keyloggers
- Phishing, spoofing, or engaging in identity theft or social engineering
- Unauthorized scanning, probing, brute-forcing, or denial-of-service attacks

Hosting illegal content including:

- Child sexual abuse material (CSAM)
- Terrorist or extremist propaganda
- Hate speech or non-consensual pornography
- Hosting adult, erotic, or pornographic material of any kind
- Operating cryptocurrency miners, blockchain nodes, or smart contract services without written approval
- Using services for criminal activity such as fraud, human trafficking, or illegal gambling
- Exceeding allocated CPU, RAM, IOPS or bandwidth limits in a disruptive manner

4. Email and Messaging Policy

The following is strictly prohibited:

- Use of purchased, harvested, or third-party mailing lists
- Sending messages without proper user opt-in and opt-out mechanisms
- Spoofing email headers, reply-to addresses, or identities
- Using Hub Hosting's infrastructure for SMTP relay abuse

Violations may result in **immediate suspension or termination**, and the domain/IP may be blacklisted.

5. Resource Usage

Clients must adhere to the resource limits of their selected service plan. Excessive or abusive usage of:

- CPU or memory
- Disk I/O operations
- Bandwidth or network throughput

... may result in **automatic throttling, temporary suspension, or permanent termination** of the affected service.

Hub Hosting reserves the right to implement automated or manual limitations to ensure service stability for all clients on web hosting servers

6. Billing Cycles

Billing terms vary by service category:

- Fully managed web hosting is billed annually by default.
- Managed VPS and Cloud Storage services are billed monthly, quarterly, semi-annually, or annually, depending on the client's selected plan.
- If a client fails to complete full payment, all associated content will be deleted 7 days after the payment due date, without further notice.

7. Security Controls

Hub Hosting maintains a security framework based on layered defense principles:

- Host-based firewalls (iptables, firewalld, nftables)
- Log-based intrusion prevention (Fail2Ban)
- Application-layer protection (Imunify360 with ModSecurity)
- PHP runtime protection (CloudLinux Proactive Defense)
- Malware scanning and heuristic WAF filters
- Data encrypted in transit using TLS 1.3**
- Data encrypted at rest using AES-256, where applicable (e.g. backups, sensitive volumes, cloud storage)

Security systems are continuously monitored and updated according to current industry best practices and regulatory requirements.

8. Data Protection & Retention

All personal data is processed in accordance with Hub Hosting's Data Protection Policy and in full compliance with **GDPR**.

- Data in transit is encrypted using TLS 1.3
- Data at rest is encrypted using AES-256, where applicable
- Client data is retained for 10 days after termination, unless otherwise required by law

Hub Hosting does not guarantee data recovery beyond this period and recommends regular offsite backups by the client.

9. Abuse Handling

Hub Hosting reserves the right to:

- Investigate any violation of this AUP
- Suspend or terminate any account without prior notice in case of severe violations
- Block malicious IPs, domains, or services
- Share evidence with law enforcement when legally obligated

Abuse reports should be submitted to: **abuse@hub-hosting.com**

Include full logs, timestamps, and relevant evidence for review.

10. Governing Law

This policy is governed by the laws of Ireland and applicable regulations of the European Union. All disputes shall fall under the exclusive jurisdiction of the courts located in Cork, Ireland.