Hub Hosting - Spam & Abuse Policy

Version: SAP-2026.1

Date: 10.02.2026

Official Legal Contact: legal@hub-hosting.com

PREAMBLE

This Spam & Abuse Policy ("Policy") defines the procedures, responsibilities, and zero-tolerance measures applied by Hub Hosting to prevent, identify, and respond to spam, network abuse, and malicious activity. This Policy is designed to align with applicable EU and Irish law and recognised good practice frameworks, including:

- Regulation (EU) 2016/679 (General Data Protection Regulation - "GDPR")
- Directive (EU) 2022/2555 ("NIS2") and any applicable Irish implementing measures once in force
- ISO/IEC 27001:2022 (Information Security Management Systems - Requirements)
- ISO/IEC 27035 series (Information security incident management), including ISO/IEC
- 27035-1:2023

1. Definitions

- "Spam" - unsolicited bulk or commercial messages sent via email or other channels.
- "Abuse" - any activity that violates applicable law, Hub Hosting's Acceptable Use Policy ("AUP"),

or interferes with network integrity or service availability.

- "Phishing" - fraudulent attempts to obtain confidential data through impersonation.
- "Malware" - software intended to damage, disrupt, or gain unauthorised access.
- "DoS/DDoS Attack" - deliberate actions intended to disrupt service availability.

2. Scope and applicability

This Policy applies to all users, clients, and third parties utilising Hub Hosting's infrastructure, including email, VPS, and web hosting services. It complements the Terms of Service ("TOS"), AUP, and Data Processing Agreement ("DPA").

3. Zero tolerance statement

Hub Hosting enforces a strict zero-tolerance policy against spam, phishing, and abuse. Any account found to be involved in such activities may be immediately suspended without notice, pending investigation and potential termination. Hub Hosting may take any additional steps permitted by law and the TOS to mitigate harm and protect its network and clients.

4. Prohibited activities

- Sending unsolicited bulk or commercial emails.
- Hosting, distributing, or linking to phishing content or malicious software.
- Launching or participating in DoS/DDoS attacks.
- Running open mail relays, proxy servers, or anonymisation networks.
- Conducting network scanning or penetration testing without prior written authorisation.
- Using Hub Hosting's infrastructure for illegal or infringing content.

5. Reporting procedure

All suspected spam or abuse incidents must be reported to: abuse@hub-hosting.com.

Reports should include:

- A description of the incident.
- Source IPs, timestamps, and relevant logs.
- Evidence of spam or network misuse.

Hub Hosting acknowledges receipt within 24 hours and initiates an investigation following its Incident Response Framework, modelled on ISO/IEC 27035 principles.

6. Investigation process

Each report is logged and classified according to severity. Steps may include:

- Initial triage within 24 hours.
- Evidence verification.
- Client notification (if applicable).
- Corrective action as soon as practicable and, where feasible, within 5 business days.

Processes are documented and reviewed as part of Hub Hosting's internal security governance.

7. Corrective actions

Depending on investigation results, Hub Hosting may:

- Suspend or terminate affected accounts.
- Restrict network access.
- Remove malicious or illegal content.
- Notify competent authorities where required by law.

No refunds on termination for abuse: Where an account is suspended or terminated due to a breach of this Policy (including spam, phishing, or other abuse), all fees are non-refundable, including any prepaid or unused services, to the extent permitted by law and the TOS.

8. False or malicious reports

Hub Hosting treats all reports confidentially and objectively. False or malicious reports made in bad faith may result in account restriction, suspension, or legal action.

9. Cooperation with authorities

Hub Hosting cooperates with relevant authorities, including:

- The Irish National Cyber Security Centre (NCSC) for cybersecurity incidents, subject to the applicable legal framework.
- The Data Protection Commission (DPC) for personal data breaches under GDPR Articles 33 and 34.

Where Hub Hosting is subject to NIS2 reporting obligations, it will submit an early warning without undue delay and, in any event, within 24 hours of becoming aware of a significant incident, followed by an incident notification within 72 hours, and further reporting as required by law. For personal data breaches, Hub Hosting will notify the relevant supervisory authority within 72 hours of becoming aware of a breach where required, and will communicate to affected individuals without undue delay where the breach is likely to result in a high risk.

10. Data handling and confidentiality

All abuse-related data and logs are handled confidentially and retained only as long as necessary for investigation, service security, or legal compliance. Reporter identities are handled in accordance with GDPR and Irish whistleblowing legislation (Protected Disclosures Act 2014 as amended).

11. Compliance statement

Hub Hosting maintains a Security and Compliance Framework aligned with ISO/IEC 27001:2022 and the ISO/IEC 27035 series for incident management. While Hub Hosting is not formally certified under ISO or SOC 2 programmes, its operational controls, monitoring, and reporting mechanisms are modelled on international best practices and reviewed annually as part of internal audit and governance.

12. Governing law and jurisdiction

This Policy is governed by the laws of Ireland and applicable EU regulations. Any disputes shall be subject to the exclusive jurisdiction of the courts of Cork, Ireland.

13. Annex reference

- Annex A: Acceptable Use Policy (AUP)
- Annex B: Terms of Service (TOS)
- Annex C: Data Processing Agreement (DPA)
- Annex D: Security & Compliance Statement