Hub Hosting - Spam & Abuse Policy

Version: HH-SAP-v2025.4

Date: 3 November 2025

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 aligned with the principles of the GDPR (EU 2016/679), the NIS2 Directive (EU 2022/2555), ISO/IEC 27001:2022, and applicable Irish cybersecurity regulations.

1. DEFINITIONS

- "Spam" – unsolicited bulk or commercial messages sent via email or other channels.
- "Abuse" – any activity that violates applicable law, Hub Hosting's AUP, or interferes with network integrity.
- "Phishing" – fraudulent attempts to obtain confidential data through impersonation.
- "Malware" – software intended to damage, disrupt, or gain unauthorized 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 utilizing Hub Hosting's infrastructure, including email, VPS, and web hosting services. It complements the Terms of Service (TOS), Acceptable Use Policy (AUP), and Data Processing Agreement (DPA).

3. ZERO TOLERANCE STATEMENT

Hub Hosting enforces a strict zero-tolerance policy against spam, phishing, or abuse. Any account found to be involved in such activities may be immediately suspended without notice, pending investigation and potential termination.

4. PROHIBITED ACTIVITIES

The following activities are explicitly prohibited:

- Sending unsolicited bulk or commercial emails.
- Hosting or distributing phishing content or malicious software.
- Launching or participating in DoS/DDoS attacks.
- Running open mail relays, proxy servers, or anonymization networks.

- Conducting network scanning or penetration testing without authorization.
- 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, aligned with ISO/IEC 27035 principles.

6. INVESTIGATION PROCESS

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

Initial triage within 24 hours.

- Evidence verification.
- Client notification (if applicable).
- Corrective action within 5 business days.

All processes are documented and reviewed as part of Hub Hosting's internal NIS2 and incident response 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.

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 or legal action.

9. COOPERATION WITH AUTHORITIES

Hub Hosting cooperates with:

- The Irish National Cyber Security Centre (NCSC) for cybersecurity incidents.

- The Data Protection Commission (DPC) for data breaches under GDPR Articles 33–34.

Serious incidents are reported to competent authorities within 24 hours of confirmation, with all necessary technical and mitigation details.

10. DATA HANDLING AND CONFIDENTIALITY

All abuse-related data and logs are handled confidentially and retained only as long as necessary for investigation or legal compliance. Reporter identities are protected under GDPR and Irish whistleblower protection laws.

11. COMPLIANCE STATEMENT

Hub Hosting maintains a Security and Compliance Framework aligned with ISO/IEC 27001:2022 and ISO/IEC 27035:2023 principles for incident management. While Hub Hosting is not formally certified under ISO or SOC 2 programs, its operational controls, monitoring, and reporting mechanisms are modelled on international best practices and reviewed annually as part of its internal audit and governance process.

12. GOVERNING LAW & 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 Statem