Stratline
NETWORKS

LEGAL DOCUMENT
SLN-LGL-002

NETWORK AND SERVICE POLICY

Acceptable Use Policy

Rules governing the use of the Stratline network, servers and IP address space, and the procedures we follow when handling abuse.

Issued by	Stratline Networks
Document	SLN-LGL-002
Version	1.0
Effective date	6 November 2026
Applies to	All customers and End Users
Website	stratline.net

Stratline Networks
stratline.net
contact@stratline.net

CONTENTS

1. Purpose and Scope
2. General Principles
3. Illegal and Harmful Content
4. Network Abuse and Security Violations
5. Email and Messaging
6. Routing and Number Resources
7. Resource Usage and Fair Use
8. Customer Security Obligations
9. Abuse Handling Procedure
10. Requests from Authorities
11. Consequences of Violations
12. Changes to this Policy

ABOUT THIS DOCUMENT

This Acceptable Use Policy (the **AUP**) protects the integrity of the Stratline network, our customers and the wider Internet. It forms part of the *Terms of Service* and applies to every customer.

It describes what you may not do with our Services, the security standards we expect, and the process and time frames we follow when we receive an abuse complaint.

Reports of abuse originating from our network should be sent to **abuse@stratline.net**.

1. Purpose and Scope

1.1 This AUP applies to all use of the Services, the Network and any IP address space or autonomous system number assigned or routed by Stratline, whether by the Customer, its End Users or any other person who gains access to the Services through the Customer.

1.2 The Customer is responsible for ensuring that its End Users comply with this AUP. Any breach by an End User is deemed a breach by the Customer.

1.3 Capitalised terms not defined in this AUP have the meanings given in the *Terms of Service*.

1.4 This AUP does not create any obligation on Stratline to monitor the content or traffic of its customers. Stratline acts as a hosting and access provider within the meaning of Articles 4 to 6 of the Digital Services Act (Regulation (EU) 2022/2065) and the German Digital Services Act (DDG) and responds to specific notices as described in section 9.

2. General Principles

2.1 The Services may only be used for lawful purposes. The Customer shall not use, or permit the use of, the Services in a manner that violates applicable law in the Federal Republic of Germany, the European Union, the country in which the Customer is established or the country in which the relevant infrastructure is located.

2.2 The Customer shall not use the Services in a manner that impairs the operation, security or integrity of the Network, the services of other customers, or any third-party network or system.

2.3 The Customer shall act in accordance with generally accepted standards of conduct on the Internet, including the Best Current Practices published by the Internet Engineering Task Force (IETF) and the RIPE community, to the extent applicable to its use of the Services.

3. Illegal and Harmful Content

3.1 The Customer shall not store, distribute, transmit, link to or make available using the Services any content that:

a. depicts the sexual abuse or exploitation of children or is otherwise unlawful under §§ 184 et seq. of the German Criminal Code (StGB), including any child sexual abuse material (CSAM), which Stratline will report to law enforcement without notice to the Customer;

b. glorifies or incites violence, constitutes incitement to hatred (§ 130 StGB), uses symbols of unconstitutional organisations (§ 86a StGB), or promotes terrorism;

c. infringes copyrights, trademarks, patents, trade secrets, design rights or other intellectual property or personality rights of third parties;

d. is defamatory, insulting or otherwise infringes the personal rights of third parties;

e. facilitates unlicensed gambling, the unlawful sale of weapons, narcotics, prescription drugs or other regulated goods;

f. constitutes or facilitates fraud, including fake shops, advance-fee fraud, investment fraud and impersonation of financial institutions or public authorities; or

g. violates applicable youth protection laws, in particular the German Interstate Treaty on the Protection of Minors in the Media (JMStV).

3.2 Stratline reserves the right to remove or block access to such content and to suspend the affected Services without prior notice where the content is manifestly unlawful or where Stratline is legally obliged to act.

4. Network Abuse and Security Violations

4.1 The Customer shall not use the Services to carry out, facilitate or attempt any of the following:

a. unauthorised access to, or use of, any system, network, account or data, including brute-force attacks, credential stuffing and exploitation of vulnerabilities;

b. port scanning, vulnerability scanning or network probing of systems for which the Customer does not hold written authorisation from the owner;

c. denial-of-service attacks of any kind, including volumetric, protocol and application-layer attacks, and the operation of so-called booter or stresser services;

d. the distribution or operation of malware, ransomware, viruses, worms, trojans, spyware or botnet command-and-control (C2) infrastructure;

e. phishing, pharming or the hosting of websites that imitate the login pages of third parties to obtain credentials;

f. the interception, monitoring or manipulation of data traffic not intended for the Customer;

g. IP spoofing, including sending packets with forged source addresses, or any traffic that is not consistent with BCP 38 / RFC 2827 source address validation;

h. the operation of open resolvers, open relays, open proxies or other services that can be misused for amplification or reflection attacks, unless adequately rate-limited and secured; or

i. cryptocurrency mining on shared virtual server products, unless expressly permitted in the Order.

4.2 Legitimate security research and penetration testing are permitted only with the prior written consent of the owner of the target system and must be conducted in a manner that does not affect the Network or third parties. The Customer shall provide evidence of such consent upon request.

4.3 Stratline may implement, without prior notice, technical measures to protect the Network, including traffic filtering, rate limiting, blackholing and the blocking of ports commonly misused for abuse (for example outbound TCP port 25 on new accounts until verified).

5. Email and Messaging

5.1 The Customer shall not use the Services to send, or to facilitate the sending of, unsolicited bulk or commercial messages (**spam**). In particular, the Customer shall:

a. only send commercial email to recipients who have given prior express consent in accordance with § 7 of the German Act Against Unfair Competition (UWG) and Art. 6 GDPR, using a confirmed (double) opt-in procedure;

b. include a functioning unsubscribe mechanism in every marketing message and process unsubscribe requests without undue delay;

c. not use purchased, rented or harvested address lists;

d. maintain correct SPF, DKIM and DMARC records and reverse DNS entries for sending infrastructure; and

e. not forge headers, sender addresses or otherwise conceal the origin of messages.

5.2 The Customer shall not cause any Stratline IP address to be listed on a recognised blocklist (including Spamhaus SBL/XBL/CSS, Barracuda and SpamCop). Where a listing results from the Customer's activity, the Customer shall bear the reasonable costs incurred by Stratline in obtaining delisting.

5.3 Stratline may require the Customer to request the activation of outbound SMTP traffic and may make such activation subject to verification.

6. Routing and Number Resources

6.1 The Customer shall only announce prefixes via BGP for which it holds the right of use, and shall maintain accurate route and route6 objects in a recognised Internet Routing Registry and valid RPKI Route Origin Authorisations.

6.2 The Customer shall not hijack prefixes, leak routes in violation of RFC 7908, announce bogon prefixes or private AS numbers, or manipulate AS paths or BGP communities to mislead other networks.

6.3 The Customer shall not use IP address space assigned by Stratline in a manner inconsistent with the justification provided, and shall not sub-assign or lease such space to third parties without Stratline's prior consent.

6.4 Geolocation, reputation and allocation data relating to Stratline address space shall not be misrepresented by the Customer.

7. Resource Usage and Fair Use

7.1 Shared resources, including CPU, storage I/O and network capacity of virtual server products, are subject to fair use. Stratline may limit the resources available to a Customer whose usage persistently and materially impairs other customers, after notifying the Customer and allowing a reasonable period to reduce usage or upgrade to a suitable product.

7.2 Traffic volumes and bandwidth limits are governed by the Order. Unless unmetered bandwidth has been expressly agreed, traffic exceeding included volumes is charged in accordance with the price list.

8. Customer Security Obligations

8.1 The Customer shall take appropriate measures to secure its systems against misuse, in particular:

a. promptly installing security updates for operating systems and applications;

b. using strong, unique passwords or key-based authentication and disabling unused services and accounts;

c. configuring firewalls to expose only the services required;

d. monitoring its systems for signs of compromise; and

e. isolating and remediating compromised systems without undue delay.

8.2 The Customer remains responsible for abuse originating from its systems even where those systems have been compromised by a third party. A compromise does not release the Customer from its obligation to remedy the abuse within the time frames set out in section 9.

9. Abuse Handling Procedure

9.1 Stratline receives abuse reports at abuse@stratline.net. Stratline's abuse contact is published in the RIPE Database (abuse-c) and in the security.txt file on Stratline's website.

9.2 Upon receipt of a credible abuse report, Stratline will forward it to the Customer's designated abuse contact. The Customer shall acknowledge receipt and take appropriate action within the response times set out in the table below, and shall inform Stratline of the measures taken.

9.3 Response times by category:

CATEGORY	EXAMPLES	CUSTOMER RESPONSE	STRATLINE ACTION IF UNRESOLVED
Critical	CSAM, active DDoS from customer systems, botnet C2, phishing of financial institutions	Immediate	Immediate suspension, without notice where required
High	Malware distribution, phishing, compromised systems actively attacking third parties, open amplifiers under attack	Within 4 hours	Null-route of affected IP addresses
Standard	Spam, port scanning, brute-force attempts, blocklisting	Within 24 hours	Suspension of affected Service after warning
Legal	Copyright notices, trademark and personality rights claims	Within 48 hours	Review and, where infringement is evident, blocking of content

9.4 Stratline may shorten these response times or act without prior notice where necessary to avert imminent danger to the Network, third parties or public safety, or where required by law or by an order of a competent authority.

9.5 Repeated abuse reports concerning the same Customer may be treated as a material breach of the Agreement entitling Stratline to terminate for good cause in accordance with the *Terms of Service*.

9.6 Stratline handles notices of allegedly unlawful content in accordance with Article 16 of the Digital Services Act. Notices should contain the information listed in Article 16(2) DSA, including the exact location (URL or IP address) of the content, an explanation of why it is considered unlawful and the identity of the notifier where required.

9.7 Where Stratline restricts content or Services on the basis of a notice, it will inform the Customer of the reasons in accordance with Article 17 DSA, unless legally prohibited or the information would compromise a law enforcement investigation.

10. Requests from Authorities

10.1 Stratline cooperates with law enforcement and regulatory authorities to the extent required by law. Requests for information or measures must be based on a valid legal basis and be submitted in the form required by law.

10.2 Stratline will inform the Customer of requests concerning its data, unless prohibited by law or by order of the requesting authority.

10.3 Stratline does not provide voluntary bulk access to customer data or traffic to any authority.

11. Consequences of Violations

11.1 In the event of a violation of this AUP, Stratline may, at its reasonable discretion and having regard to the severity of the violation and the Customer's legitimate interests, take one or more of the following measures:

a. issue a warning and request remediation within a reasonable period;

b. filter, rate-limit or block specific traffic, ports or protocols;

c. null-route individual IP addresses or prefixes;

d. suspend the affected Services in whole or in part in accordance with the *Terms of Service*;

e. terminate the Agreement for good cause; and

f. report criminal conduct to the competent authorities.

11.2 The Customer shall reimburse Stratline for reasonable costs incurred as a result of a violation for which the Customer is responsible, including staff time for the handling of abuse at a rate of EUR 95 per commenced hour, costs of delisting and any fines or third-party claims, in accordance with the indemnification provisions of the *Terms of Service*.

11.3 Measures taken under this AUP do not entitle the Customer to service credits or a reduction of Fees.

12. Changes to this Policy

12.1 Stratline may update this AUP to reflect changes in the law, industry practice or threats to the Network. Material changes will be notified to Customers in Text Form at least thirty (30) days before they take effect, except where an immediate change is required by law or to respond to a new security threat.

12.2 The current version of this AUP is published on Stratline's website.

Stratline Networks · stratline.net · contact@stratline.net
End of document · SLN-LGL-002 v1.0