



Arelion acceptable use policy

Customer is expected to use the Service(s) in accordance with reasonable industry standards and shall be responsible for its use of the Service as well as the activities of any end user or third-party that uses or accesses the Services through Customer. Customer's use of the Service(s) provided pursuant to the Agreement shall be subject to this Acceptable Use Policy ("AUP" or "Policy"). Customer shall not:

1. Use the Service for the transmission, distribution, receipt or retrieval of any information, data, or other material or in a manner that violates any applicable law, statute, ordinance, order or regulation or in a manner that would expose Arelion to criminal or civil liability;
2. Use the Service in a manner that infringes any third party's copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy;
3. Use the Service to commit any act, or to transmit or distribute, any material or information that is defamatory, abusive, libellous, threatening, harassing or obscene;
4. Use the Service to send, distribute, receive, collect or redirect unsolicited emails, chain letters, mailbombs or SPAM (unsolicited bulk email and/or unsolicited commercial email);
5. Use the Service in a manner that interferes with, disrupts, compromises the normal functioning of, or causes an excessive or disproportionate load on Arelion's or any third party's network, system, account, computing facility, website, or equipment (e.g., distributed denial of service, SYN flood or similar attacks that seek to overburden a recipient, network, system or equipment by sending mass amounts of traffic or data with the intent to compromise, interfere with or disable the recipient or target);
6. Use the Service to commit, or attempt to commit, acts of unauthorized relays through any third party systems;
7. Use the Service to exploit vulnerabilities in hardware or software for malicious purposes or in connection with spoofed or forged IP addresses, traffic or electronic mail;
8. Use the Service to operate open relay/unsecure mail servers which provide SMTP or similar functionality to third parties;



9. Use the Service to distribute viruses, Trojan horses, worms, malware, corrupted data or programs or other similar harmful or deleterious software, information, data, materials or programming routines (including port scanning);
10. Use the Services in an effort to gain unauthorized access to, or attempt to interfere with or compromise the integrity or security of, any network, system, account, computing facility, website or equipment, including any attempt to probe, scan, test the vulnerability of, penetrate or circumvent the security of a network, system, account, computing facility, website or equipment;
11. Use the Service to monitor any data, communications or information on any network, system, account, computing facility, website or equipment without appropriate authorization; or
12. Use the Service to introduce false or misleading information into the Internet or any other network (e.g., incorrect or deceptive routing information or spoofed IP addresses), to announce a network or autonomous system or IP address space not properly registered with and/or assigned to the user by an appropriate authority, or in connection with hijacked IP address space or a hijacked ASN.

Customer agrees and acknowledges that the violation of this AUP by Customer's subscribers, end-users or customers or any third-party that gains access to the Service through Customer shall be deemed to be a violation by Customer of the AUP. Customer is solely responsible for any use of the Service provided by Arelion and nothing in this Policy obligates Arelion to monitor, edit, manage or censor Customer's use of the Services. Arelion makes no guarantee regarding, and assume no liability for, the security and integrity of any data, material or information a Customer transmits via the Service or over the Internet.

Arelion reserves the right to rely on information disclosed, reported or received from third parties, including without limitation from organizations that track spam and other cyber abuses and threats, in determining whether Customer's use of the Service(s) is in compliance with or in violation of this AUP. Arelion agrees to use reasonable efforts to notify Customer by electronic mail of any violations of the AUP and to give Customer an opportunity to correct any violations before taking action, provided that Arelion shall reserve the right to suspend or block Service without notice in cases where the operation, security, or integrity of Arelion's or a third-party' network, system, account, computing facility, website, or equipment is threatened, disrupted or compromised by Customer's violation of the AUP, in cases where Customer's violation of this AUP involves illegal activities or could subject Arelion to criminal or civil liability, in cases where Customer is unavailable or there have been repeated AUP violations, or in cases involving, for example,





UCE/SPAM, mail relaying, alteration of IP address information, denial of service attacks, or the announcement of unregistered or unauthorized networks or IP space.

The list of unacceptable uses set forth above is not exhaustive and Arelion reserves the right to take action in order to address any use of the Service that Arelion determines to be in breach of this Policy or that may be harmful to the Arelion network, its customers, peers, or other users of the Internet. Arelion reserves the right to modify this Policy at any time by posting the updated version on its website.

