

SYRINGA NETWORKS, LLC ACCEPTABLE USE POLICY

This Acceptable Use Policy (this "Policy") is an integral part of SYRINGA NETWORKS, LLC's ("SYRINGA's") Standard Terms and Conditions and Master Services Agreement and is specifically incorporated into such Agreements. For purposes of this Policy, "Customer" shall be defined to include SYRINGA'S Customers and also a Customer's end users and account holders. This Policy is subject to change with notice by publication on this web site: (http://www.syringanetworks.net/resources/acceptable_use_policy/); Customers are responsible for monitoring the identified web site for changes.

This Policy is designed to help protect SYRINGA, SYRINGA's Services, our Customers, and the Internet community in general from irresponsible, inappropriate, and illegal activities. The Internet is a conglomeration of online databases operated by distinct entities having no business or legal relationship with SYRINGA. SYRINGA does not control the content of Internet data accessed via its Services. Customers are solely responsible for any value or reliance they place on information they obtain via the Internet or the Services. Information derived from the Internet is provided "as is" and is accessed at the Customer's own risk. SYRINGA warrants only that it shall, subject to the terms and conditions of this Policy and its Service Agreement, provide Customer access to the Internet and makes no other warranties.

Customer understands that if it fails to provide any information necessary for the initiation or continued provision of Services, or provides inaccurate information, and such failure or inaccuracy results in installation delays or necessitates that SYRINGA complete additional work, Customer will be invoiced SYRINGA's costs for each such failure in an amount up to \$250 per instance.

- 1. PROHIBITED ACTIVITIES.** The actions described below are strictly prohibited under this Policy. These examples are not representative of actual Customer experiences and are provided solely for guidance to Customers. If a Customer questions whether a contemplated use or action is permitted, it is Customer's responsibility to determine whether the use is permitted by contacting SYRINGA at abuse@syringanetworks.net.
 - **ILLEGAL ACTIVITY.** SYRINGA's Services shall be used in compliance with all applicable laws at all times. Accordingly, SYRINGA strictly prohibits the use of Services for the transmission, distribution, retrieval, or storage of any information, data or other material in violation of any applicable law or regulation (including, where applicable, any tariff or treaty). This prohibition includes, without limitation, the use or transmission of any data or material protected by copyright, trademark, trade secret, patent or other intellectual property right without proper authorization and the transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory or otherwise unlawful.
 - **UNAUTHORIZED ACCESS/INTERFERENCE.** A Customer may not attempt to gain unauthorized access to or attempt to interfere with or compromise the normal functioning, operation or security of, any portion of SYRINGA's network. A Customer may not use the Services to engage in any activities that may interfere with the ability of others to access or use the Services or the Internet. A Customer may not use the Services to monitor any data, information or communications on any network or system without appropriate authorization. A Customer may not attempt to gain unauthorized access to the user accounts or passwords of other Users.
 - **UNSOLICITED COMMERCIAL EMAIL/SPAMMING/MAILBOMBING.** SYRINGA's Services may not be used to transmit unsolicited commercial e-mail messages or deliberately send excessively large attachments to one recipient. In addition, SYRINGA prohibits the

use of the Services for any "spamming" or "mailbombing" activities. Use of the service of another provider to send unsolicited commercial email, spam or mailbombs, to promote a site hosted on or connected to SYRINGA's network, is similarly prohibited. Likewise, a Customer may not use the Services to collect responses from mass unsolicited e-mail messages. SYRINGA may in its sole discretion rely upon information obtained from anti-spamming organizations (including for example and without limitation spamhaus.org, spamcop.net, sorbs.net, and abuse.net) as evidence that a Customer is an active "spam operation" for purposes of taking remedial action under this Policy.

- **SPOOFING/FRAUD**. SYRINGA prohibits Customers from intentionally or negligently injecting false data into the Internet, for instance in the form of bad routing information (including but not limited to the announcing of networks owned by someone else or reserved by the Internet Assigned Numbers Authority) or incorrect DNS information. A Customer may not attempt to send e-mail messages or transmit any electronic communications using a name or address of someone other than the Customer for purposes of deception. Any attempt to impersonate someone else by altering a source IP address information or by using forged headers or other identifying information is prohibited. Any attempt to fraudulently conceal, forge or otherwise falsify a Customer's identity in connection with use of the Service is also prohibited.
 - **USENET POSTINGS**. All postings to USENET groups must comply with that group's charter and other policies. Customers are prohibited from cross posting to unrelated news groups or to any news groups where the post does not meet that group's charter. Continued posting of off-topic messages, including commercial messages (unless specifically invited) is prohibited. Disrupting newsgroups with materials, postings or activities that are (as determined by SYRINGA in its sole discretion) frivolous, unlawful, obscene, threatening, abusive, libelous, hateful, excessive or repetitious, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, FAQ or charter.
 - **OTHER PROHIBITED ACTIVITIES**: Intentionally transmitting files containing a computer virus or corrupted data; repeatedly exceeding any agreed upon bandwidth limitations on the Customer's account; attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document use of SYRINGA's Services; advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this Policy, which includes the facilitation of the means to deliver unsolicited commercial email; any activity that disrupts, degrades, harms or threatens to harm SYRINGA's network or Services; any use of another party's electronic mail server to relay email without express permission from such other party; any other inappropriate activity or abuse of the Services (as determined by SYRINGA in its sole discretion), whether or not specifically listed in this Policy.
2. **CUSTOMER RESPONSIBILITIES**. Customers who provide services to their own users must (1) affirmatively and contractually incorporate this Policy into agreements with their end users; (2) take steps to ensure compliance by their users with this Policy; (3) maintain valid postmaster and abuse addresses for their domains; and (4) provide SYRINGA with a 24/7 contact address for purposes of security and abuse issues. In most cases, SYRINGA will notify our Customer of complaints we receive regarding an alleged violation of this Policy. Customer agrees to promptly investigate all such complaints and take all necessary actions to remedy any violations of this Policy. SYRINGA may inform the complainant that our Customer is investigating the complaint and may provide the complainant with the necessary information to contact the Customer directly to resolve the complaint.

3. **SYSTEM SECURITY.** Security is the sole responsibility of the end user of all devices connected to SYRINGA's network. All networks connected to SYRINGA Services should have security applied to mitigate threats and equipment being compromised. Customer is solely responsible for the selection, implementation and maintenance of security features for protection against unauthorized or fraudulent use of the Service. Customer is entirely responsible for maintaining the confidentiality of password and account information, as well as the security of their network. Customer agrees to immediately notify SYRINGA of any unauthorized use of its account or the Service, if a Service-related device is stolen, or any other breach of security known to it. Customer must notify SYRINGA if it becomes aware of any violation of this Policy by any person, including other users that have accessed the Service through Customer's account. In addition, all Customers of the SYRINGA Network are responsible for notifying SYRINGA immediately if they become aware of any other event that may negatively affect SYRINGA's network, including, but not limited to, any threatened "denial of service" attack, unauthorized access, or other security events. Until Customer provides any such notification, Customer will be liable for all use of the Service using a stolen device and any stolen, fraudulent, or unauthorized use of the Service whether or not it involves a stolen device.
4. **INDEMNIFICATION.** Customer specifically agrees to defend, indemnify, and hold harmless SYRINGA, its agents, officers, directors, employees, successors, and assigns, from any claim, loss, or damage, including costs and attorneys' fees, arising out of or related to act or omission of a Customer, including without limitation the Customer's causation of damages or injury, directly or indirectly, to any party.
5. **COOPERATION WITH INVESTIGATIONS.** SYRINGA will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity on the SYRINGA Network. SYRINGA reserves the right to disclose Customer information to the extent authorized or required by applicable law or regulation.
6. **SYRINGA's RIGHTS.** SYRINGA expressly reserves the right, at its discretion, to pursue any remedies that it believes are warranted which may include, but are not limited to, the issuance of written or verbal warnings, filtering, blocking, suspending, or terminating accounts, billing Customer for administrative costs and/or reactivation charges or bringing legal action to enjoin violations and/or to collect damages, if any, caused by Customer violations. Such actions may be taken by SYRINGA without notice to Customer. SYRINGA does not have any liability to any party, including Customer and Customers subscribers or end users, for any violation of this Policy.
7. **JURISDICTION.** This Policy shall be construed under the laws of the State of Idaho and Idaho Courts shall have jurisdiction over SYRINGA and its Customers.
8. **VOIP USAGE.** Unauthorized or excessive use of VoIP Services beyond that normally experienced by typical business customers violates this AUP and may cause congestion issues and interference with SYRINGA's network and third-party networks with whom SYRINGA may connect for call initiation and completion services. SYRINGA reserves the right to review Customers' accounts at any time for potential abuses of this AUP or usage in excess of Customer's agreed use. SYRINGA may determine abnormal or abusive usage based on comparisons to usage patterns of other customers. If SYRINGA

determines that Customer has violated this AUP or otherwise exceeded Customer's expected usage, SYRINGA may invoice Customer, and Customer shall pay for such excessive use at the then-current rates established by SYRINGA. In addition to excessive use charges, if SYRINGA identifies excessive or abusive traffic patterns, SYRINGA reserves the right to change Customer's applicable rate plan or suspend or terminate Service with or without notice.

Last Modified: 03/12/2020