

SVIC
ACCEPTABLE USE POLICY

As a provider of Internet access and other Internet related services, M & R Johns, Inc DBA SVIC [SVIC] offers its Customers the means to acquire and disseminate a wealth of public, private, commercial and non-commercial information. SVIC has developed this Acceptable Use policy [AUP] which supplements and explains certain terms of each Customer's respective Agreements with SVIC and sets forth certain Customer rights and obligations which govern the use of SVIC's services. SVIC reserves the right to revise, amend, or modify this AUP at any time and in any manner. Any revision, amendment, or modification will be posted at:
<http://www.svic.net>.

Please read this policy prior to accessing the Service. All users of the Service must abide by this AUP. Your violation of this AUP may result in the immediate suspension or termination of either your access to the Service and/or your SVIC account. This AUP should be read in conjunction with our Installation Agreement, Customer Agreement, Privacy Policy, and other applicable policies.

By using the Service, you agree to abide by, and require others using the Service via your account to abide by the terms of this AUP. You should consult this document regularly to ensure that your activities conform to the most recent version. **IF YOU DO NOT AGREE TO ABIDE BY THESE TERMS, YOU SHOULD IMMEDIATELY STOP THE USE OF THE SERVICE AND NOTIFY SVIC SO THAT YOUR ACCOUNT MAY BE CLOSED.**

SVIC cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that Customers may acquire through the Internet, with the exception of its proprietary websites. Customers must exercise their best judgment in relying on information obtained from the Internet and also should be aware that some material posted to the Internet is sexually explicit or otherwise offensive. Because SVIC cannot monitor or censor the Internet and will not attempt to do so, SVIC cannot accept any responsibility for injury to its Customers that results from inaccurate, unsuitable, offensive, or illegal Internet communications.

Because the Internet is neither more nor less secure than other means of communication including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised, SVIC recommends that its Customers assume that all of their on-line communications are not secure. SVIC assumes no responsibility for the security of information transmitted through SVIC's facilities.

SVIC will not intentionally monitor private electronic mail messages sent or received by its Customers unless required to do so by law, governmental authority, or when public safety is at stake. SVIC may however, monitor its service electronically to determine that its facilities are operating satisfactorily. Also, SVIC may disclose information, including but not limited to, information concerning a Customer, a transmission made using SVIC network, or a website, in order to comply with a court order, subpoena, summons, discovery request, warrant, statute, regulation, or governmental request. SVIC may disclose Customer information or information transmitted over its network where necessary to protect SVIC and others from harm or where such disclosure is necessary to the proper operation of the system.

The following are prohibited activities and if Customer engages in any of them, then such action will be a violation of this AUP and Customer will be in breach of its Agreement with SVIC:

a. Spamming: SVIC may immediately terminate any account that it determines, in its sole discretion, is transmitting or is otherwise connected with any "spam" or other unsolicited bulk email. In addition, if actual damages cannot be reasonably calculated, SVIC reserves the right to block, reject, or remove what it considers in

its sole discretion to be "spam" or other unsolicited bulk email from the Service and SVIC shall have no liability for blocking any email considered to be "spam."

b. Intellectual Property Violation: Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including copyrights, trademarks, service marks, trade secrets, software piracy, and patents held by individuals, corporations, or other entities and also, engaging in activity that violates privacy, publicity, or other personal rights of others. SVIC is required by law to remove or block access to Customer content upon receipt of a proper notice of copyright infringement. SVIC reserves the right to terminate the privileges of Customers who commit repeat violations of copyright laws.

c. Materials Harmful to Minors: Using SVIC's network to advertise, transmit, store, post, display, or otherwise make available illegal pornography or material that is harmful to minors. SVIC is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through SVIC's network.

d. Defamatory or Abusive Language: Using SVIC's network as a means to transmit or post defamatory, harassing, abusive messages or language which threatens bodily harm or destruction of property, or inappropriate language directed to minors.

e. Forging or Impersonating of Headers: Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.

f. Illegal or Unauthorized Access to Other Computers or Networks: Accessing or collecting illegally or without authorization computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (i.e., port scan, stealth scan, or other information gathering activity).

g. Reselling the Services: Reselling the services is not permitted.

h. Distribution of Internet Viruses, Worms, Trojan Horses, or Other Destructive Activities: Distributing information regarding the creation of and/or sending internet viruses, worms, Trojan Horses, pinging, flooding, mailbombing, unsolicited commercial email or bulk mail, or denial of service attacks. Also, activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service, or equipment. It is Customer's responsibility to ensure that their network is configured in a secure manner. A user may not, through action or inaction, allow others to use their network for illegal or inappropriate activities.

i. Facilitating a Violation of this AUP: Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of means to spam, initiation of pinging, flooding, mailbombing, denial of service attacks, piracy of software.

j. Export Control Violations: Exporting encryption software over the Internet or otherwise, to points outside the United States.

k. Usenet Groups: Posting to newsgroups with content that violates this AUP. SVIC reserves the right not to accept such postings when it has actual knowledge that the content violates this AUP. The continued posting of off-topic articles is prohibited. Commercial advertisements are off-topic in most newsgroups, especially regional groups not specifically named for such. The presence of such articles in a group is not indicative of the group's "intended" use. Please familiarize yourself with basic Usenet netiquette before posting to a newsgroup. SVIC considers "multiposting" to 10 or more groups within a two week sliding window to be excessive. SVIC servers currently limit the number of allowable "cross-posts" to 9. SVIC may not cancel messages other than its own messages. Customer may cancel posts forged in that Customer's name. SVIC may cancel any postings which violate this AUP.

l. Excessive Use: Using Customer's account for high volume use is prohibited without SVIC authorization. The Service is intended for periodic, active use of email, newsgroups, file transfers, Internet chat, games, and browsing the World Wide Web. It is not designed for excessive uploading and downloading. If a customer has excessive use to where it affects the bandwidth or speed of other customers, SVIC maintains the

right, at its own discretion, to terminate or slow a customer's connection following any extended period of high volume use, as determined by SVIC.

m. Hosting Websites: Hosting Websites is not allowed on this network without written permission from SVIC.

n. Hacking: Accessing any of SVIC's equipment, computers or network to read, alter, or modify configuration or firmware.

o. Other Illegal Activities: Engaging in activities that are determined to be illegal, including fraudulent offers to sell or buy products, items, or services and advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.

p. Other Activities: Engaging in activities, whether lawful or unlawful, that SVIC determines to be harmful to its Customers, operations, reputation, good will or customer relations.

When SVIC becomes aware of any of the described prohibited activities or activities that violate any law, it may take any action to immediately stop such activity including, but not limited to, terminating service, issuing written and/or verbal warnings, removing information, shutting down a website, implementing screening software designed to block offending transmissions, suspending or denying access to the Internet, or take any other action it deems appropriate. Customers are encouraged to provide SVIC with all available information regarding a suspected violation of this AUP.