Southwest Arkansas Telephone Cooperative, Inc. / SWAT FIRST
Acceptable Use Policy

Introduction

Southwest Arkansas Telephone Cooperative, Inc. / SWAT FIRST and its affiliates and subsidiaries ("SWAT," "we," or "us") appreciate the opportunity to provide you with a connection to the Internet. This Acceptable Use Policy, together with the terms and conditions for your Internet service, provide guidelines for your conduct on the Internet as a SWAT residential or business customer.
By using SWAT's Internet services, you agree to comply with this Acceptable Use Policy and to remain responsible for all activity originating from your account. We reserve the right to modify this Acceptable Use Policy from time to time, effective when posted to www.swatfirst.com. Your use of the Internet services after changes to the Acceptable Use Policy are posted shall constitute acceptance of any changed or additional terms.

Scope

This Acceptable Use Policy applies to SWAT's data services that provide (or include) access to the Internet, including but not limited to dedicated data center services, or that are provided over the Internet (collectively "Internet services").
For ease of reference, this policy addresses the following topics:
Section 1: Prohibited Activities
Section 2: Consequences for Activities in Violation of this Policy
Section 3: Privacy
Section 4: Account Usage
Section 5: Copyright Complaints

Section 1: Prohibited Activities

General Prohibitions: It shall be a violation of this Acceptable Use Policy to use our Internet service in any way that is unlawful, harmful to or interferes with use of our network or systems, or the network of any other provider, violates the policies of any network accessed through our Internet service, interferes with the use and enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.
If you have any questions regarding this Acceptable Use Policy, or wish to report a suspected violation of this policy, you may contact smarthub@swat.coop.

Intellectual Property Rights: SWAT's Internet services shall not be used to host, publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of SWAT or any individual, group or entity, including but not limited to rights protected by any intellectual property right.

Child Pornography: SWAT's Internet services shall not be used to host, publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store

child pornography. Suspected violations of this prohibition may be reported to applicable law enforcement agency.

E-mail and Related Services: Spam/E-mail or Usenet abuse is prohibited using SWAT's Internet services. Examples of Spam/E-mail or Usenet abuse include, but are not limited to the following activities:
Sending a harassing e-mail, whether through content, frequency or size
Sending the same (or substantially similar) unsolicited e-mail message to an excessive number of recipients
Sending multiple unwanted e-mail messages to the same address, or sending any e-mail that provokes a complaint to SWAT from the recipient
Continuing to send e-mail to a specific address after the recipient or SWAT has requested you to stop
Falsifying your e-mail or IP address, or any other identification information
Using e-mail to originate chain e-mails or originate or forward pyramid-type schemes
Using a mail server to relay or intercept e-mail without the express permission of the owner
Sending e-mails, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of SWAT's network or of the networks with which SWAT interconnects, by virtue of quantity, size or otherwise
Sending unsolicited mass or commercial e-mail ("spamming") for any purpose whatsoever. Mass or commercial e-mail may be sent only to recipients who have expressly requested receipt of such e-mails, by the sending of an e-mail request to the person performing the mass or commercial mailings. This exchanging of requests, acknowledgements, and final confirmations (commonly referred to as a "double opt-in" process) must be adhered to in its entirety for any mass or commercial e-mail to be considered "solicited." If you send mass or commercial e-mail, you must maintain complete and accurate records of all e-mail subscription requests, specifically including the e-mail and associated headers sent by you. Subscriptions that do not have a specific recipient-generated e-mail request associated with them are invalid, and are strictly prohibited. A violation of the CAN-SPAM Act will be considered a violation of this policy.
Newsgroup spamming or cross-posting the same (or a substantially similar) article to multiple Newsgroups; Many Newsgroups prohibit posting of commercial advertisements or solicitations. Usenet policy prevents off-topic posting of articles. You are required to comply with both Newsgroup(s) and Usenet's policies. We reserve the right to restrict access to any Newsgroups.
Using an Internet Relay Chat ("IRC") bot, or violating any policy of an IRC server, including use of IRC-based telephony and video conferencing. It is your responsibility to determine the acceptable use policies for any IRC server to which you connect. We reserve the right to restrict access to IRC services.

Hacking and Attacks: Hacking or attacking is prohibited using SWAT's Internet services. Hacking is any unauthorized attempt to monitor access or modify computer system information or interference with normal system operations, whether this involves SWAT equipment or any computer system or network that is accessed through our service. Attacking is any interference with Internet service to any user, host or network, including mail bombing, ping flooding, broadcast attempts or any attempt to overload a system to interrupt service. Examples of hacking and attacking include, but are not limited to the following:
Satan or port scans, full, half, FIN or stealth (packet sniffing)
SubSeven port probes
BO scans or attacks
Mail host relaying, mail proxying, or hi-jacking
Telnet, FTP, Rcommands, etc. to internal systems
Attempts to access privileged or private TCP or UDP ports

Multiple and frequent finger attempts
User ID/Password cracking or guessing schemes
Virus, worms and Trojan horse attacks
Smurf, teardrop and land attacks
Participation in botnets, including but not limited to, spam e-mail messages, viruses, computer/server attacks, or committing other kinds of crime and fraud

Network Management: To preserve the integrity of our network, we implement reasonable network management practices to ensure that all customers have an enjoyable experience using the Internet. SWAT's Internet services shall not be used in a manner that is excessive or unreasonable with respect to frequency, duration or bandwidth consumption when compared to the predominant usage patterns of other customers on a similar service plan or in your geographic area. As technology and customer usage change, SWAT reserves the right to adjust its determination of excessive or unreasonable use. SWAT reserves the right to terminate service that it determines is excessive or unreasonable or to implement charges for excessive or unreasonable usage in its sole discretion. In the event SWAT determines, in its sole discretion, a customer's usage is excessive or unreasonable, SWAT will make reasonable efforts to provide customer with notice prior to taking any action regarding customer's service.

Section 2: Consequences for Activities in Violation of this Policy

Suspension and Termination: SWAT has the right, in its sole discretion, with or without notice, to suspend or terminate your account when you engage in any conduct that violates SWAT's Terms and Conditions (which includes this policy) We will make reasonable efforts to contact you if you are in jeopardy of suspension or termination; however, to protect our network and our customers, we reserve the right to block you first and subsequently contact you. We also reserve the right to cancel e-mail messages and/or restrict the size of e-mail distribution lists.

Charges: You agree to be responsible and pay for any activities that result in damages and/or administrative costs to us or our customers. These damages include, but are not limited to the following: system shut downs, retaliatory attacks or data flooding, and loss of peering arrangements.

Section 3: Privacy
Any information transmitted through the Internet, including information about you, can be intercepted by unwanted third parties. There is no guarantee that you or SWAT can prevent this. We provide certain security measures to reduce the risk that information about you is intercepted by others.
In an effort to protect your privacy, we:
use security techniques designated to prevent unauthorized access of information about you.
will honor your requests to remove your name from e-mail solicitation lists.
do not collect personally identifiable information about you unless you provide it to us.
do not sell the names and addresses of our customers, or visitors to our sites, to others without providing information of that disclosure when the personally identifiable information is collected.
do not provide customer information to other companies with which we do business without an understanding that they will respect your privacy.
For more information about SWAT's privacy policies, please see SWAT's Privacy Statement at www.swatfirst.com

Section 4: Account Usage

Usage
Your SWAT Internet account may only be used according to your service plan. If your account is not a Business account, then it may not be used to provide dedicated services such as e-mail, gaming, or streaming audio or video servers. Dedicated accounts may include but are not limited to Ethernet Internet and Dedicated Internet services. SWAT reserves the right to restrict access to sites that are being used for commercial use.

Passwords
You are solely responsible for maintaining the confidentiality of your account I.D. and passwords. Subscribers should not provide their login and password for use by others outside of their immediate business or household. You must notify us immediately if your account I.D. and/or password have been lost, stolen, or otherwise compromised. Simultaneous use of our service by multiple users with a single login and password is not allowed. Reselling or sharing, in whole or in part, access to your Internet account or Internet connectivity without our expressed written consent is prohibited.

Internet Software
SWAT is not a software licensor, and the license agreement for your Internet software is not a part of your service agreement with us. This means that your software license agreement may either remain in effect or terminate independently from your Internet service.
We are not responsible for technical support or the integrity of any files or software that you obtain from any other source. It is your responsibility to determine whether any software that you intend to use, including any program that you intend to download from the Internet, is compatible with your computer and can be installed correctly and safely. We strongly recommend that you review the documentation accompanying any software before you attempt to install it.

Section 5: Copyright Complaints
The Digital Millennium Copyright Act of 1998 ("DMCA") provides recourse for owners of copyrighted material who believe their rights under U.S. copyright law have been infringed on the Internet or other telecommunications networks.
As a provider of transitory digital communications, SWAT's activities are typically protected by a safe harbor provision of the DMCA (see 17 U.S.C. 512 (a)). SWAT is therefore not obligated to respond to a copyright owner (or the owner's agent) nor does SWAT have a duty to remove or disable access to material transmitted, routed or connected to the SWAT network(s) that is initiated and/or directed by an individual user.