

**Standing Rock Telecom, Inc.**  
**ACCEPTABLE USE POLICY**

**INTRODUCTION**

This Acceptable Use Policy ("AUP") is a legally binding agreement between you ("Customer(s)" or "You") and Standing Rock Telecommunications, Inc. and its affiliates ("Standing Rock" or "Service Provider") for use of Service Provider's broadband Internet access services ("Services"). Standing Rock is a 100 percent tribally-owned company, founded by the leadership of the Standing Rock Sioux Tribe ("Tribe"). Nothing in this policy shall constitute a waiver of the sovereign immunity of the Tribe.

Customer must be at least 18 years old to establish an account. By establishing an account and/or by using or activating Services, Customer agrees to be bound by this AUP and to use Services in accordance with this AUP and other Service Provider policies posted on Service Provider's website, including but not limited to Service Provider's Terms of Service, Open Internet Policy, DMCA Policy, and Privacy Policy, which are available on the Standing Rock website under Legal. In the event of any conflict between such terms and this AUP, the terms of this AUP shall govern and control. Service Provider may modify this AUP from time to time.

This AUP is intended to help enhance the use of the Internet by preventing unacceptable use and it is designed to help protect Service Provider's assets, the integrity of Service Provider's network, the assets of Service Provider's customers, and the Internet community from irresponsible or illegal activities of Service Provider's customers and users. These activities may disrupt or degrade Services; pose a threat to Service Provider's assets; expose Service Provider (or other providers of Internet services) to claims of civil or criminal liability or other legal sanctions. Because of various conventions used in the industry (including blocking, filtering, and blacklisting), these activities may impair Service Provider's ability to interconnect with other providers of Internet services. These activities may relate to the content stored or transmitted by Customers or authorized users or to the nature of the transmissions themselves, such as sending large numbers of unsolicited messages ("spam"). Customers are responsible for avoiding the prohibited activities and strictly following the AUP terms set forth herein.

PLEASE READ THIS POLICY CAREFULLY BEFORE ACCESSING OR USING THE SERVICES. BY ACCESSING OR USING THE SERVICES, YOU AGREE TO BE BOUND BY THIS POLICY. IF YOU DO NOT WISH TO BE BOUND BY THIS AUP, YOU MAY NOT ACCESS OR USE THE SERVICES.

**GENERAL POLICY**

Service Provider reserves the right in its sole discretion to deny or restrict your use of the Services, or immediately to suspend or terminate your Services, if the use of your Services by You or anyone using the Services, in our sole discretion, violates the Terms of Service or other Service Provider policies, is objectionable or unlawful, interferes with the functioning or use of the Internet or Service Provider's network by Service Provider or other users, or violates the terms of this AUP.

## **ILLEGAL AND PROHIBITED USE**

The following actions, content, and/or practices are examples of illegal and/or prohibited conduct, which may result in the termination of Customer's account. Customers in violation of this AUP may also be subject to any appropriate legal action and/or consequences. Service Provider reserves the right to cooperate with legal authorities and/or injured third parties in the investigation of any suspected illegal activity or civil wrong.

The Services shall not be used in connection with any criminal, civil, or administrative violation of any applicable local, state, and provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule. By using Services, Customer represents and warrants to Service Provider that Customer is not a resident of any country, or affiliated with, any of organization prohibited to do business within the United States, as defined by the Office of Foreign Assets Control within the United States Department of the Treasury. Further, Customer represents that Customer will not download or otherwise use the Services in Cuba, Iran, North Korea, Sudan and Syria or to destinations that are otherwise controlled or embargoed under U.S. law, as modified from time to time by the Departments of Treasury and Commerce.

Services shall not be used to host, post, transmit, or re-transmit any illegal content or materials.

Service Provider has a zero tolerance policy regarding use of Services to engage in inappropriate conduct with a minor (anyone under 18 years of age). Customer shall not knowingly collect or solicit personal information from a minor without the express consent of the parent or guardian of the minor, nor shall Customer use Services to harm or intimidate a minor. Service Provider complies with all federal and state laws pertaining to the protection of minors.

Other activities or use of Services that Service Provider considers to be a violation of this AUP are as follows, but are not limited to:

- posting or transmitting information or communications that, whether explicitly stated, implied, or suggested through use of symbols, are obscene, indecent, pornographic, sadistic, cruel, or racist in content, or of a sexually explicit or graphic nature, or which espouse, promote or incite bigotry, hatred, terrorism or racism, or which might be legally actionable for any reason;
- posting, transmitting, downloading or viewing any material whatsoever pornographic in nature involving actual images of children or minors or digitally or otherwise artificially created or manipulated images of children or minors, or any material whatsoever that may be deemed obscene under applicable law;
- accessing or attempting to access the accounts of others, to spoof or attempting to spoof the URL or DNS or IP addresses of Service Provider or any other entity, or attempting to penetrate or penetrating security measures of Service Provider or other entities' systems ("hacking") whether or not the intrusion results in corruption or loss of data;
- introducing viruses, locks, keys, bombs, worms, harmful code, Trojan horses, cancelbots, or any other harmful features on the Internet;

- violating Service Provider's or any third party's copyright, trademark, proprietary or other intellectual property rights, including trade secret rights;
- using any name or mark of Service Provider, its parent, affiliates or subsidiaries, as a hypertext link to any Web site or in any advertising publicity or other commercial manner;
- using the Services or the Internet in a manner intended to threaten, harass, intimidate, abuse, slander, libel, defame, or terrorize;
- making false or unverified complaints against any Service Provider subscriber, or otherwise abusing any of Service Provider's complaint response procedures;
- collecting or storing personal data about other users;
- impersonating any person or entity or forging anyone else's digital or manual signature;
- attempting to violate, whether indirectly or not, this AUP;
- reselling of service provided by Service Provider;
- using the Services to transmit, retransmit, distribute, post, or store any material that in the judgment of Service Provider is threatening, libelous, defamatory, or otherwise objectionable, including but not limited to child pornography and advocating unlawful activity against any persons, animals, governments or businesses; harassment of users, employees, or of others will not be tolerated;
- actions and/or Services prohibited by federal, state and local law;
- distributing, posting, copying or disseminating copyrighted material, including but not limited to movies and/or music;
- inhibiting any other person's use of the Services provided by Service Provider;
- participating in illegal gambling, lottery or other similar activities;
- transmitting, conducting, participating in, or otherwise facilitating scams, including pyramid schemes, other illegal schemes, or any schemes for making money fast;
- making fraudulent offers; and
- attempting to access the accounts of others or other computers and/or networks to penetrate security measures, whether or not the intrusion results in damage.

Service Provider reserves the right to limit, to restrict, and to prohibit Services that it provides to Customers, as Service Provider determines necessary. The restrictions stated here apply to all users unless otherwise specifically documented.

## **EMAIL / SPAM**

Any user of Service Provider Services found to be actively distributing or engaged in the mass distribution of unsolicited emails without consent of the intended receiver may have their account(s) terminated and all future access to Service Provider's Services and network revoked. Violation of the CAN-SPAM Act of 2003, the Electronic Mail Act of Illinois (Public Act 91-0233), or any other state or federal law regulating e-mail services, constitutes an automatic violation of this AUP and Service Provider reserves the right to seek damages and other available relief against Customer, as applicable.

Service Provider reserves the right to limit the file size of individual email mailboxes at its sole discretion. Individual email mailboxes found over the limit will be subject to deletion without notice. Deleted email will not be restored or saved. Service Provider reserves the right to limit the maximum transfer limit of any one message in its sole discretion. Service Provider reserves the right to reject or filter email based on source address and content. Examples are, but are not limited to, virus filtering and blocking open relay mail servers. Service Provider will not make back-ups of a customer's email.

The Services may not be used to transmit, retransmit, or distribute by email or any other method any material that violates any condition of this AUP in the sole judgment of Service Provider. Violations of the AUP are not limited to the following, but the following activities are considered by Service Provider to be a violation of this AUP and You may not use the Services or any equipment or software provided by Service Provider:

- to spam or to send unsolicited email of a personal, bulk, or commercial nature email, , including, without limitation, bulk mailings of commercial advertising, informational announcements, charity requests, political or religious messages, petitions for signatures, and any chain mail related materials, except to those who have requested such emails via a confirmed opt-in subscription process maintained by You;
- to sending bulk (i.e., twenty-five or more recipients) emails without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- to send bulk emails in quantities that exceed standard industry norms, or that create the potential for disruption of the Service Provider's network or of the networks with which Service Provider interconnects;
- to conduct "mail bombings" (e.g., to send more than ten copies of the same or substantially similar message, or to send very large messages or files, with the intent of disrupting a server or account);
- to use distribution lists containing addresses that include those who have opted out;
- to send e-mail or other messages to someone who has indicated that he or she does not want to receive messages from You;
- to use redirect links in unsolicited commercial e-mail to advertise a website or service;
- to send multiple email messages or to retransmit email messages for the purpose of misleading recipients as to the origin by using another computer, without authorization;

- to send emails that do not accurately identify the sender, the sender's return address, the email address of origin, or other information contained in the subject line or header;
- to forge headers or identifiers in order to disguise the origin of e-mail;
- to use IP addresses that the Customer does not have a right to use;
- to use another Internet site's mail server to relay mail without the express permission of the owner of that Internet site;
- to maintain a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- to send messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of Service Provider's Services or the Internet (e.g., through language, frequency, size or otherwise);
- to intercept, redirect or otherwise interfere or attempt to interfere with e-mail intended for other parties;
- to post a single message, or messages to online forums or newsgroups, that could reasonably be expected to provoke complaints;
- to post messages to, to cancel, or to supersede messages on an online forum or newsgroup in a manner that violates the rules of the forum or newsgroup or that contain forged header information;
- to email the same or similar messages to one or more newsgroups (also known as "cross-posting" or "multiple posting");
- to knowingly delete any author attributions, legal notices, or proprietary designations or labels in a file that the user mails or sends;
- to use, distribute, advertise, transmit, or otherwise make available any software program, product, or service that is designed to violate this AUP or the AUP of any other provider of Internet service, including, but not limited to, the facilitation of the means to spam;
- to collect or receive responses from unsolicited e-mail messages (even if such e-mail was sent from accounts on other Internet service providers or e-mail Services) that violate the agreement or this AUP or the terms of use under the other Internet service provider or email service from which it was sent;
- to solicit email that contains material that otherwise violates this AUP or any email that falsifies the address or other information;
- to harvest e-mail addresses or personal information of other Service Provider subscribers or the subscribers of any other network;
- to send or forward make-money-fast schemes or chain/pyramid scheme letters (whether or not the recipient requests it);
- to send email containing false or misleading statements, claims, or representations; and
- to use email or the Internet in violation of federal law or the rules of the Federal Communications Commission.

## **SERVING**

Serving of any kind is NOT allowed without express written consent from Service Provider. Consent should be given in a separate service contract and should be producible by the Customer upon request from Service Provider. Serving constitutes: Email servers, Web and HTTP servers, FTP servers, IRC servers, and other listening Internet services.

## **UNAUTHORIZED SHARING**

You agree not to allow others to use any of the Services provided including, but not limited to, sharing your account user name and password, dial-up access, or broadband access via any type of networking device (router, gateway, wireless access point, etc.). You may at your own risk and responsibility permit other members of your household to access the Services and utilize some networking devices approved by the provider for use within your household only. You as the account holder shall ensure that other such users are aware of and comply with these terms of use, and you agree to be held responsible for any activity or use of the Services on that account, whether or not authorized by you.

## **OTHER SERVICES**

Other Services not specifically listed in this AUP, but that are provided by Service Provider are also governed by this AUP.

## **COMPLIANCE WITH THE AUP OF UPSTREAM PROVIDERS**

The AUP of Service Provider's upstream providers also bind Service Provider's users. An "upstream provider" is any company that may provide Service Provider with bandwidth and/or other services.

## **SYSTEM AND NETWORK SECURITY**

Violations of system or network security are prohibited and may result in criminal and civil liability. Service Provider will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- port scanning, probes, data capture, denial of service, access of restricted systems;
- attempted access of systems not previously given access to;
- anything deemed "hacking" or "cracking" to the systems, network or users;
- unauthorized access to or use of data, including any attempt to circumvent user authentication or security of any host, network, or account (hacking, cracking, port scans, or flood pings);
- unauthorized monitoring of data or traffic;
- interfering with service to any user, host, system or network;
- conducting denial of service attacks;

- any attempt to disrupt service including, but not limited to, distributing or introducing viruses, worms, or other harmful software;
- access by using artificial means, involving software, programming, or any other method.

Customer is solely responsible for the security of any device connected to Services, including any data stored on that device. Service Provider's Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of Service Provider's or another party's server, network, personal computer, network access or control devices, software or data, or other system, or to attempt to do any of the foregoing.

### **COPYRIGHT INFRINGEMENT / REPEAT INFRINGER POLICY**

Service Provider respects the intellectual property rights of third parties, including those granted under the US copyright laws, and the interests of its subscribers and content providers on the Internet. You may not store material of any type or in any format on, or disseminate such material over, Service Provider's systems or servers in any manner that constitutes an infringement of third party intellectual property rights, including rights granted under the US copyright laws. In accordance with the Digital Millennium Copyright Act ("DMCA") and other applicable law, it is the policy of Service Provider to terminate, in appropriate circumstances, the Services provided to any subscriber or account holder who is deemed to infringe third party intellectual property rights, including repeat infringers. Appropriate circumstances may exist where: (i) a subscriber or account holder has been found by a court of competent jurisdiction to have infringed the copyrights of a third party on two or more occasions, i.e., a repeat infringer, (ii) where a valid, effective and uncontested notice has been provided to Service Provider alleging facts which are a violation by the subscriber or account holder of Service Provider's DMCA Policy prohibiting infringing activity involving Service Provider systems or servers, or (iii) in other cases of repeated flagrant abuse of access to the Internet (e.g., willful commercial piracy or malicious attempts to destroy the value of copyrighted works). In addition, Service Provider expressly reserves the right to terminate or suspend the Services of any subscriber or account holder if Service Provider, in its sole judgment, believes that circumstances relating to the infringement of third party intellectual property rights warrant such action. These policies are in addition to and do not affect or modify any other rights Service Provider may have under law or contract.

You represent that you are not a specifically designated individual or entity under any US embargo or otherwise the subject, either directly or indirectly (by affiliation, or any other connection with another party) to any order issued by any agency of the US Government limiting, barring, revoking or denying, in whole or in part your US export privileges. You agree to notify Service Provider if you become subject to any such order. You agree to obtain all required permissions if you use the Service to receive, upload, download, display, distribute, or execute software or perform other works protected by intellectual property laws including copyright, trademark, trade secret and patent laws. You agree to cooperate with Service Provider and provide requested information in connection with all security and use matters.

## **CUSTOMER RESPONSIBILITY**

Customers are responsible for protecting their accounts and must take steps to ensure that others do not gain unauthorized access to customer's account or misuse Service Provider's Services. You agree to notify Service Provider promptly if you suspect any unauthorized use of the Services or of your UserID. Customer remains solely and fully responsible for the content of any material posted, hosted, downloaded, uploaded, created, accessed, or transmitted using Services. Customers should NOT: share account information, leave username and passwords in the open, or "save" user names or passwords. Customers are strongly encouraged to use anti-virus software and personal firewalls. Service Provider takes no responsibility and assumes no liability for any material created or accessible on or through Service Provider's network(s) using Services, or for any mistakes, defamation, slander, libel, omissions, falsehoods, obscenity, pornography, or profanity Customer may encounter.

## **ADMINISTRATIVE DISCRETION**

Service Provider administrators, staff, and executives have sole and final discretion over all aspects of service, the network, and this AUP. Service Provider reserves the right to terminate any account or service without cause or prior notice.

## **VIOLATIONS AND MONITORING**

Service Provider does not intend to, but reserves the right to, monitor any Services on or within our network(s). Reporting violations, attempted violations, complaints, and/or concerns should be addressed to Standing Rock Telecom, Inc. via email at **DMCANotice@standingrocktelecom.com**.

When reporting anything to Service Provider please include:

- the Internet protocol address used to commit the alleged violation;
- the date, time and time zone of such violation
- evidence of the violation, including, if applicable, full headers from emails, firewall logs, traffic dumps (example, the \*.enc files generated by Network Ice's Black Ice program or "hex" dump from any other firewall or IDS system) or information pertaining to the events in question.

Do not send excerpted parts of a message; sending the entire message with full headers helps prevent misunderstandings based on incomplete information or information taken out of context.

Service Provider has sole judgment and discretion on how we enforce this AUP. Guidelines as to punishment and legal action will be within the Service Provider's legal department and administrative department discretion.

## **REVISIONS**

Changes to this AUP are considered effective immediately and it is the Customer's responsibility to stay current. Service Provider can make changes to the AUP at any time without notice. Changes to this document will be available on Service Provider's web page. Service Provider may, but is not required to, monitor your compliance, or the compliance of other subscribers and users, with this AUP.