

HIGHWINDS NETWORK GROUP, INC.
ACCEPTABLE USE POLICY

1. Terms of Use.

a. In General. All Highwinds customers are responsible for reviewing and complying with this Acceptable Use Policy (the "Policy"). Highwinds customers who provide services to their own customers or other end users are responsible for compliance with the terms of this Policy by their customers or end users and must take steps to ensure compliance by their users with this Policy. For the purposes of this Policy, "Customer" means each Highwinds customer to whom Highwinds provides services, and all employees, agents, and third parties (including customers and end users) to whom Customer makes Highwinds services available.

b. General Prohibitions. The actions described below are defined by Highwinds as "network abuse" and are strictly prohibited under this Policy. The examples named below are not exhaustive and are provided solely for guidance to Customers; Highwinds reserves the right to determine that any conduct that is or could be harmful to Highwinds' network, Customers or users is in violation of this Policy and to exercise any or all of the remedies contained in this Policy. If any Customer is unsure of whether a contemplated use or action is permitted, it is Customer's responsibility to determine whether the use is permitted by contacting Highwinds via email at cdn-abuse@highwinds.com. In general, Highwinds Customers may not use Highwinds' network, machines, or services in any manner that:

- violates any applicable law, regulation, treaty, or tariff, including, but not limited to, data privacy laws;
- violates the acceptable use policies of any networks, machines, or services that are accessed through Highwinds' network;
- infringes on the intellectual property rights of Highwinds or others;
- violates the privacy of others;
- involves the resale of Highwinds' products or services, unless specifically documented in a separate written agreement or in the initial Customer contract with Highwinds;
- involves deceptive online marketing practices including, without limitation, practices that violate the United States Federal Trade Commission's guidelines for proper online marketing schemes;
- violates any specific instructions given by Highwinds for reasons of health, safety or quality of any other telecommunications services provided by Highwinds or by reason of the need for technical compatibility of equipment attached to the Highwinds network;
- materially affects the quality of any telecommunications services provided by Highwinds; or
- otherwise violates this Policy.

c. Specific Prohibitions. Other expressly prohibited activities include, but are not limited to, the following:

- unauthorized use (or attempted unauthorized use) or sabotage of any computers, machines or networks;
- attempting to interfere with or denying service to any user or host (e.g. denial of service attacks and/or DNS spoofing attacks);
- falsifying user identification information;
- introducing malicious programs into Highwinds' network or servers (e.g. viruses, worms, Trojan horses, etc.);
- scanning the networks of others for vulnerabilities without authorization;
- executing any form of network monitoring (e.g. using a packet sniffer) or otherwise engaging in any monitoring or interception of data not intended for the Customer without authorization;
- attempting to circumvent Customer authentication or security of any host, network, or account ("cracking") without authorization;
- using any program/script/command, or sending messages of any kind, designed to interfere with a third party customer terminal session, via any means, locally or via the Internet;
- "phishing," that is, simulating communications from and/or the website or other service of another entity in order to collect identity information, authentication credentials, or other information from the legitimate users of that entity's service;
- "pharming," that is, using malware, DNS cache poisoning or other means to redirect a user to a website or other service that simulates a service offered by a legitimate entity in order to collect identity information, authentication credentials, or other information from the legitimate users of that entity's service;
- transmitting or receiving, uploading, using or reusing material which is abusive, indecent, defamatory, obscene or menacing, or in breach of copyright, confidence, privacy or similar third party rights;
- furnishing false or incorrect data on the signup form;
- using the services in excess of any specified bandwidth limitation for Customer's user account;
- advertising, transmitting or otherwise making available any software, program, product or service that is designed to violation this Policy;
- attempting to circumvent or alter the process or procedures to measure time, bandwidth utilization, or other methods to document "use" of Highwinds' products and services;
- falsifying header information or user identification information;
- attempted or successful security breaches or disruption of Internet communication including, but not limited to, accessing data of which Customer is not an intended recipient or logging into a Highwinds server or account that Customer is not expressly authorized to access;
- hijacking of IP space;
- sending unsolicited ("opt-out") bulk email;
- collecting responses from mass unsolicited email messages;

- deliberately sending excessively large attachments to one email recipient;
- transmitting unsolicited commercial email messages;
- maintaining an open mail relay and/or an open proxy; and
- collecting email addresses from the Internet for the purpose of sending unsolicited bulk email or to provide collected addresses to others for that purpose.

d. Filters. Highwinds reserves the right to install and use, or to have Customer install and use, any appropriate devices to prevent violations of this Policy, including devices designated to filter or terminate access to the Highwinds services.

e. Digital Millennium Copyright Act. It is Highwinds' policy to respond expeditiously to claims of intellectual property infringement. Highwinds will promptly process and investigate notices of alleged infringement and will take appropriate actions under the Digital Millennium Copyright Act ("DMCA") and other applicable intellectual property laws. Upon receipt of notices complying or substantially complying with the DMCA, when it is under its control, Highwinds will act expeditiously to remove or disable access to any material claimed to be infringing or claimed to be the subject of infringing activity and will act expeditiously to remove or disable access to any reference or link to material or activity that is claimed to be infringing. Highwinds will terminate access for Customers who are repeat infringers. If you believe that a copyrighted work has been copied and is accessible on our site in a way that constitutes copyright infringement, you may notify us by providing our registered copyright agent with the following information:

- electronic or physical signature of the person authorized to act on behalf of the owner of the copyright interest;
- a description of the copyrighted work that you claim has been infringed;
- a description of where the material that you claim is infringing is located on the site;
- your address, telephone number, and e-mail address;
- a statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law; and
- a statement by you, made under penalty of perjury, that the above information in your notice is accurate and that you are the copyright owner or authorized to act on the copyright owner's behalf.

Notices of claimed infringement should be directed to cdn-dmca@highwinds.com. When Highwinds removes or disables access to any material claimed to be infringing, Highwinds may attempt to contact the Customer who has posted such material in order to give that Customer an opportunity to respond to the notification. Any and all counter notifications submitted by the Customer will be furnished to the complaining party. Highwinds will give the complaining party an opportunity to seek judicial relief in accordance with the DMCA before Highwinds replaces or restores access to any material as a result of any counter notification.

f. Cooperation with Law Enforcement. Highwinds will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal

or inappropriate activity. Highwinds reserves the right to disclose Customer information to the extent authorized or required by federal or state law. Without limiting the foregoing, in those instances involving child pornography, Highwinds complies with all applicable federal and state laws and provides notice to the National Center for the Missing and Exploited Children or other designated agencies, including, without limitation, the Internet Watch Foundation, and Highwinds removes all content for which removal is requested by such agencies.

g. Impending Security Event Notification. Customer is responsible for notifying Highwinds immediately if Customer becomes aware of an impending event that may negatively affect the Highwinds network. This includes, without limitation, extortion threats involving threat of “denial of service” attacks, unauthorized access, or other security events.

h. Configuration. Customer is responsible for configuring its own systems to provide the maximum possible accountability. Highwinds shall not be liable for any damage caused by such system configurations regardless of whether such configurations have been authorized or requested by Highwinds. For example, Customer should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. Customer should also configure its Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange, and should generally present header data as clearly possible. As another example, Customer should maintain logs of dynamically assigned IP addresses. Customer is responsible for educating itself and configuring its systems with at least basic security. Should systems at Customer’s site be violated, Customer is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) server, Customer is responsible for re-configuring the system to stop the abuse.

i. Downstream Users. Highwinds Internet transit and colocation Customers who provide those services to their own users must affirmatively and contractually pass on the restrictions of this Policy to its users and take steps to ensure compliance by their users with this Policy, including, without limitation, termination of the user for violations of this Policy. Highwinds Internet transit and colocation Customers who provide services to their own users also must maintain valid postmaster and abuse addresses for their domains; comply with all applicable Internet RFCs; maintain appropriate reverse DNS information for all hosts receiving connectivity through Highwinds' network for which DNS responsibility has been delegated to the Customer; maintain accurate contact information with the InterNIC and any other appropriate domain, IP and AS registrars; take reasonable steps to prevent IP spoofing by their users and downstream customers, including, without limitation, using IP unicast reverse-path forwarding ("uRPF") wherever appropriate and using IP address filtering wherever appropriate; provide a 24/7 contact address to Highwinds for dealing with security and abuse issues; and act promptly to ensure that users are in compliance with Highwinds' Policy. When Highwinds receives a complaint regarding an alleged violation of this Policy by Customer’s user, Highwinds may notify the Customer of such complaint, inform the complainant that Customer is investigating the complaint and provide the complainant with the necessary information to contact Customer directly to resolve the complaint.

j. Email. In connection with any email transmitted or received via the Highwinds network, servers or services, the following actions are prohibited:

- using email to engage in harassment, whether through language, frequency, or size of messages. Continuing to send someone email after being asked to stop is considered harassment;
- using email to disrupt (e.g., mail bombing, "flashing," etc.);
- originating email with falsified header information;
- originating email with falsified or obscured information (e.g., encoded or "obfuscated URLs") designed to hinder identification of the location of what is advertised;
- originating chain letters, pyramid schemes, and hoaxes;
- using another party's email server to relay email without express permission from such other party;
- using the Highwinds or Customer account to collect replies to messages sent from another provider that violate these rules or those of the other provider; and
- using Highwinds services in connection with or in support of the running of a mail server without a license to run such a server in any jurisdiction where such license is required.

k. Bulk Email. Customers sending bulk email using Highwinds services may only engage in such activity through the use of "closed-loop opt-in" lists. Such Customers who send bulk email through "closed-loop opt-in" lists must have a method of confirmation or verification of subscriptions and be able to show evidence of subscription for users who complain about receiving unsolicited email. Sending unsolicited ("opt-out") bulk email is prohibited and is grounds for termination of those services to Customers who engage in the practice. Sending "opt-out" bulk email from another provider advertising or implicating, directly or indirectly, the use of any service hosted or provided by Highwinds, including without limitation, email, web, content distribution, FTP, and DNS services, is prohibited. Customers may not advertise, distribute, or use software intended to facilitate sending "opt-out" email or harvest email addresses from the Internet for that purpose. In addition, Customers may not sell or distribute lists of harvested email addresses for the purpose of "opt-out" email. Customers who provide or make use of a service employing referral IDs will be considered responsible for unsolicited bulk email sent by members of the referral ID service that makes reference to services hosted by Highwinds. Customers who engage in the practice of unsolicited bulk email, as set forth above, from Highwinds accounts will be charged the cost of labor to respond to complaints, with a minimum charge of \$200. Customers listed on an industry-recognized spam abuse list will be deemed to be in violation of this Policy.

l. Usenet. Customers should be familiar with the workings of Usenet by reading FAQs regarding Usenet at <http://www.faqs.org/faqs> before becoming active participants. Highwinds places the following restrictions on newsgroup postings by its Customers:

- no illegal content, including pyramid/Ponzi schemes, infringing materials, or child pornography, is permitted;

- all postings, including, without limitation, cross-postings, should conform to the various conventions, charters, guidelines and local culture found in each respective newsgroup and Usenet as a whole. For example, commercial advertising is typically off-topic and/or a violation of the charter in most Usenet newsgroups;
- postings, materials or activities that are determined by Highwinds, in its sole discretion, to be frivolous, unlawful, obscene, threatening, abusive, libelous, hateful, excessive or repetitious are prohibited, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, FAQs or charter;
- posting 20 or more copies of the same article in a 45-day period ("spamming") or continued posting of off-topic articles, including commercial messages (unless specifically invited), is prohibited. Customers who engage in spamming using Highwinds accounts will be charged the cost of labor to issue cancellations and respond to complaints, with a minimum charge of \$200. Customers who engage in spamming from another provider advertising or implicating, directly or indirectly, the use of any service hosted or provided by Highwinds, including without limitation email, web, FTP, and DNS services, is prohibited and is grounds for termination of those services to those users;
- excessive crossposting; and
- posting articles with falsified header information is prohibited. "Munging" header information to foil email address harvesting by "spammers" is acceptable provided that a reasonable means of replying to the message originator is given. Use of anonymous remailers is acceptable, so long as the use is not otherwise a violation of this Policy.

Customers may not issue cancellations for postings except those which they have posted themselves, those which have headers falsified so as to appear to come from such Customer, or in newsgroups where they are the official moderator.

m. The World Wide Web and FTP. Highwinds reserves the right to require that sites using web or FTP space which receive high amounts of traffic be moved to other servers. Web pages and FTP files may not contain any material, text, or images, whether hosted on Highwinds servers or "transclusioned" (images from another site displayed on the page), that violate or infringe any copyright, trademark, patent, statutory, common law, or proprietary rights of others. Web pages and FTP files may not contain links that initiate downloads of copyright-infringing or other illegal material.

n. Routing Protocols and Route Exchange. In the event Highwinds learns that Customer is sending excessive or unnecessary route publications, Highwinds reserves the right to limit the number or routes that will be accepted.

o. Internet Relay Chat. Using IRC bots is prohibited. Flooding, cloning, spoofing, harassment, or otherwise hindering the ability of others to properly use IRC is prohibited. Impersonating other users, advertising, and spamming via IRC is prohibited. IRC services that are serving as command and control channels for bots are prohibited, and any violation shall

subject Customer to filtering and blocking by Highwinds within 24 hours of Highwinds learning of such violation. Highwinds is not obligated to provide notice of such action to Customer.

p. Servers and Proxies. Customers may not run on Highwinds' servers any program that makes a service or resource available to others, including, but not limited to, port redirectors, proxy servers, chat servers, MUDs, file servers, and IRC bots. Customers may not run such programs on their own machines connected to the Highwinds network in order to make such services or resources available to others; a dedicated access account is required for such purposes. Customers are responsible for the security of their own networks, machines and accounts, including, without limitation, maintaining confidentiality of password and account information. Highwinds will assume neither responsibility nor accountability for failures or breach of Customer-imposed protective measures, whether implied or actual. Abuse that occurs as a result of a compromised Customer's system or account, such as when a system becomes infected with a worm or Trojan horse program as a result of an Internet download or the execution of an email attachment, may result in suspension of services or account access by Highwinds. Any programs, scripts, or processes that generate excessive server load on Highwinds servers are prohibited, and Highwinds reserves the right to terminate or suspend any such program, script, or process.

q. Dialup Connections. Customers may not run programs or configure machines in such a way as to keep a dialup connection active when not in use or otherwise bypass automatic disconnection for inactivity, unless they have a dedicated Internet access account. Customers may not have multiple simultaneous connections with a single dialup account. Highwinds reserves the right to impose restrictions on or terminate accounts deemed to be in violation of these conditions. Highwinds' dialup access servers will disconnect after 30 minutes of inactivity and after 12 hours of continuous access.

r. Storing Files. The storage of any program, utility or file on Highwinds' servers, the use of which would constitute a violation of this Policy, is prohibited. For example, it is a violation to store hacker scripts, IRC bots, or spamming software on Highwinds' servers.

3. Privacy. Because the Internet is an inherently open and insecure means of communication, any data or information a user transmits over the Internet may be susceptible to interception and alteration. Subject to its online Privacy Policy, available at <http://www.highwinds.com/legal>, Highwinds make no guarantee regarding, and assumes no liability for, the security and integrity of any data or information a Customer transmits via our services or over the Internet, including any data or information transmitted via any server designated as "secure." Customers should not have an expectation of privacy in any content, including accounts of files transmitted through Highwinds' services.

4. Violations. Highwinds has absolute discretion in determining whether a Customer's activities or use of Highwinds' services are in violation of this Policy. In the event of the breach of or failure to comply with this Policy by any Customer, Highwinds expressly reserves the right, at its discretion, to pursue any remedies that it believes are warranted, which may include, but are not limited to, suspension or termination of the provision of a Highwinds service or services

and any other remedies available at law or equity. Such actions may be taken by Highwinds without notice to Customer.

5. Modifications to Policy. This Policy is subject to change with notice by publication on this web site; Customers are responsible for monitoring this web site for changes. This Policy was last updated on January 23, 2008. While Highwinds uses reasonable efforts to provide accurate and up-to-date information on this web site, Highwinds makes no warranty or representation as to its accuracy. Moreover, information that may have been accurate at the time of posting may have changed and therefore may no longer be accurate or in effect. Highwinds undertakes no duty to update such information.

6. Additional Terms and Conditions. All use of the Highwinds network and services is subject to the terms and conditions of any agreements entered into by such Customer and Highwinds. This Policy is incorporated into such agreements by reference.

7. Contact Information. To contact us with questions or comments regarding this Policy, or to report claimed violations of this Policy, please email cdn-abuse@highwinds.com.