



Internet Acceptable Use Policy

This Acceptable Use Policy specifies the actions prohibited by CONXX, Inc. ("CONXX") to users of the Internet Services provided through CONXX or its underlying carrier partners. CONXX reserves the right to modify the Policy at any time, effective upon posting of the modified Policy to this URL: <http://www.CONXX.net/terms>

Illegal Use

The CONXX Internet Service may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

In general, CONXX Customers may not use CONXX's network, machines, or services in any manner which:

- 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 which are accessed through CONXX's network;
- Infringes on the intellectual property rights of CONXX or others;
- Violates the privacy of others;
- Involves the resale of CONXX's products or services, unless specifically documented in a separate written agreement or in the initial Customer contract with CONXX;
- 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 CONXX for reasons of health, safety or quality of any other telecommunications services provided by CONXX or by reason of the need for technical compatibility of equipment attached to the CONXX Network;
- Materially affects the quality of any telecommunications services provided by CONXX; or
- Otherwise violates this Acceptable Use Policy.

Prohibited activities also include, but are not limited to:

- 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);
- Introduction of malicious programs into the network or Server (e.g. viruses, worms, Trojan horses, etc.);
- Attempting to circumvent Customer authentication or security of any host, network, or account ("cracking");
- Monitoring or scanning the networks of others without permission;
- Hijacking of IP space;
- 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 Server or account that Customer is not expressly authorized to access;
- Executing any form of network monitoring (e.g. packet sniffer) which will intercept data not intended for the Customer;
- 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;
- Maintaining an open mail relay and/or an open proxy;
- Collecting email addresses from the Internet for the purpose of sending unsolicited bulk email or to provide collected addresses to others for that purpose;
- 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; or
- Attempting to circumvent or alter the process or procedures to measure time, bandwidth utilization, or other methods to document "use" of CONXX's products and services

System and network security

Violations of system or network security are prohibited, and may result in criminal and civil liability. CONXX 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:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

Email

Users shall not use another site's mail server to relay mail without the express permission of the site. Users are prohibited from sending unsolicited email messages ("Spamming"), including but not limited to:

- Posting the same or similar messages to one or more Usenet or other newsgroups, forums, email mailing lists or other similar groups or lists;
- Posting any Usenet or other newsgroup, forum, email mailing list or other similar group or list articles which are off-topic or otherwise violate the rules of the charter or other owner-published FAQ or description of the group or list;
- Sending unsolicited email, including commercial advertisements and informational announcements, to Internet users, or any unsolicited email that could reasonably be expected to provoke complaints.
- Using email to engage in harassment, whether through language, frequency, or messages. Continuing to send someone email after being asked to stop is considered harassment.
- Sending email with falsified or obscured header or information designed to hinder the identification of the location of what is advertised.
- Collecting replies to either (i) unsolicited email messages or (2) messages that were either sent through another provider which violate these rules or those of the other provider.

Users who send bulk email to "opt-in" list must have a method of confirming or verifying subscriptions and be able to show evidence of subscriptions for users who complain about unsolicited email. CONXX's receipt of complaints from internet users related to emails received due to Users use of "opt in" list shall be a violation of this AUP.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE POLICY, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A CONXX CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THE POLICY BY SUCH CUSTOMER OR END USER.

Complaints regarding illegal use of system or network security issues, SPAM or USENET abuse must be sent to abuse@CONXX.net

For live security incidents, please contact CONXX Internet Abuse Investigations at 1-800-XXX-XXXX (Hours 24x7).