

Internet Access Services

Acceptable Use Policy

DayStar Communications ("Provider") has established this Acceptable Use Policy ("AUP") to advise the users of its network and services ("Users") of the acceptable and prohibited uses of its network and services (collectively, the "Services"). Provider's network and services must be used only for lawful purposes and for purposes consistent with this AUP. Examples of prohibited use identified in this AUP are non-exclusive and are provided as guidelines to Provider's Users.

All Users of the Services are required to comply with this AUP, as well as all applicable laws and regulations.

The AUP has been developed to facilitate the following objectives:

- To clearly establish and identify the guidelines under which the Services may be used;
- To ensure the integrity and reliability of the Services;
- To generally define those actions which Provider considers abusive.

Violation of this AUP is strictly prohibited. In the event of any actual or potential violation or conduct that is otherwise improper or illegal, Provider reserves the right to suspend or terminate any or all the Services. In the event Provider elects to terminate any or all parts of the Services, any penalties associated with early termination of service will apply.

Users who violate this AUP also may incur criminal or civil liability. Provider may refer violators to civil or criminal authorities for prosecution, and will cooperate fully with applicable government authorities in connection with civil or criminal investigations of such violations.

Provider reserves the right to modify this AUP at anytime effective upon written notification to customers or posting of a modified policy on Provider's website. It is the responsibility of each User periodically to check Provider's website for updates to this Policy.

1. USER RESPONSIBILITIES

Provider provides access to many areas of the Internet. Provider does not review, pre-screen, censor or edit the content of any communications transmitted through or via the Services. Provider does not review, censor or edit the content of any communications accessible via other networks that may be connected to Provider. Provider does not make any promise, nor does it have any obligation to monitor or police activity occurring via the Services and will have no liability to any party, including Users, for any violation of the AUP. Provider, however, has the right in its sole discretion to remove any content that in Provider's judgment does not comply with this AUP or is otherwise objectionable, harmful, inaccurate, or illegal. Provider is not responsible for any failure or delay in removing such content.

Each User is responsible for providing Provider with reasonable assistance in its investigation and resolution of issues, problems and/or complaints arising out of the use of the Services. Each User is responsible for immediately reporting to Provider any network issue which could compromise the stability, service, security or any use of the Services, including, without limitation, the unauthorized use of a User's authentication information. Each User is entirely responsible for maintaining the confidentiality of its authentication information and account information and is responsible for all activities that occur under its account. Therefore, authentication information should not be disclosed to unauthorized third parties.

2. ABUSE

The following actions are considered by Provider to be "Abuse" and are strictly prohibited.

- Any conduct, which could be construed to violate the general norms or etiquette of the Internet Community, regardless of whether detailed in this AUP. Provider reserves the right, in its sole discretion, to determine whether any particular User conduct violates such norms.
- Resale of the Services without Provider's express written consent.
- Using the Services to transmit any material (by e-mail, uploading, posting or otherwise) that threatens or encourages bodily harm or destruction of property;
- Using the Services to harm, or attempt to harm, minors in any way.

- Using the Services to engage in deceptive or unfair online marketing, including without limitation, making fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters."
- Using the Services to falsify the identity or contact information of any person.
- Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document use of the Services.
- Creating active full-time connection on dial up accounts by using artificial means.
- Using the Services to harvest, collect, or attempt to collect personal information from anyone without their knowledge or consent, including without limitation, knowingly soliciting or collecting personal information from a minor (anyone under eighteen (18) years old) without appropriate prior verifiable parental consent. Personal information includes but is not limited to, name, address, phone number or e-mail address.
- Using the Services to record the conversations or communications of other people without their consent.
- Using the Services for any activity, which adversely affects the ability of other people or systems to use the Services, including without limitation, disruption or interference with other Provider users and denial of service attacks against another network host or user.
- Violating any system or network security measures including but not limited to engaging in:
 - Unauthorized access or use of Provider's or a third party's network, data, or information; including any attempt to probe, scan or test the vulnerability of a system or network or to breach security authentication measures without express authorization of the owner of the secured network;
 - Unauthorized monitoring of Provider's or third party's data, systems or network traffic;
 - Interference with a third party's use of Provider's network or service, including without limitation, mailbombing, flooding, and deliberate attempts to overload a system.
 - Forging of any header or any part of the header information in any e-mail or newsgroup posting or taking any action in order to obtain services to which such user is not otherwise entitled.
 - Activities that cause interference with a third party's ability to connect to the Internet or provide services to Internet users
- Security of a User's network and systems is the sole responsibility of the User. Any firewalls, firewall configurations, routers and router configurations or any other equipment owned, implemented and maintained by the User (collectively "User Equipment") are the responsibility of the User. Provider is not responsible for any loss of data as a result of a User's selection or method of security or routing configurations. In the event that a User requests that Provider perform any work or maintenance on User Equipment, Provider shall not be responsible for any damages, including loss of data, resulting from such work or maintenance.

3. EMAIL & SPAMMING

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.
- Violating any state or federal laws regulating the use of e-mail, including without limitation, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.

Users who send bulk email to an "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. Provider'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.

4. ILLEGAL OR UNLAWFUL USE

Users shall not create, transmit, upload, post, distribute, facilitate distribution in any manner or store any information, content, or material, including without limitation, text, sounds, data, software, images, communications, or other information which:

- infringes any copyright, trademark, trade secret, patent, or other proprietary rights of any third party, including, without limitation, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorized transmittal of copyrighted software, music or movies. Sharing or downloading copyrighted materials via a peer-to-peer network is strictly prohibited;
- is obscene, indecent, immoral, or pornographic;
- is libelous, defamatory, hateful, constitutes an illegal threat or abuse, is invasive of another's privacy or publicity or harasses or intimidates an individual or a group of individuals on the basis of race, age, ethnicity, sexual orientation, gender, religion or disability or otherwise violates the legal rights of others;
- violates export control laws or regulations;
- encourages conduct that would constitute a criminal offense or give rise to civil liability under local, state, federal or international laws;
- is false, inaccurate or misleading; or
- contains any viruses, Trojan horses, worms, time bombs, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or personal information.
- otherwise violates any applicable law, rule or regulation.

5. WEB PROHIBITED ACTIVITIES

Users are expressly prohibited from engaging in the any of the following web-related activities.

- Exploiting or attempting to exploit any scripts presented on web pages.
- Excessive use of bandwidth by utilizing programs, scripts of commands to abuse a website.
- Operating a robot on a web page following request by the website that the behavior cease.
- Configuring a website to act maliciously against visitors to the website.
- "Walking" a database to collect data contained therein.
- Attempting to intercept, redirect or otherwise interfere with communications intended for others.

6. Users are prohibited from falsifying user information provided to Provider or to other users in connection with use of the Services.

7. Users are prohibited from engaging in any of the foregoing activities by using the service of another provider, but channeling such activities through an account, remailer, or otherwise through the Provider Services or using an account as a maildrop for responses or otherwise using the services of another provider for the purpose of facilitating the foregoing activities if such use of another party's service could reasonably be expected to adversely affect the Services.

8. Provider considers the above practices to constitute abuse of its service. Engaging in one or more of these practices may result in immediate termination of a User's access to the Services. Users shall be charged an administrative fee of \$500 for each incident in violation of this AUP. A violation of this AUP by someone having only indirect access to the Services through a customer or other user will be considered a violation by the customer or other user whether or not with the knowledge or consent of the customer or other user. Provider receives complaints directly from internet users, through internet organizations, and through other parties.

9. Provider shall not be required to determine the validity of complaints received before taking action under this AUP. Provider reserves the right in its sole discretion to determine whether duplicative or mass e-mail messages are "unsolicited." A complaint from the recipient, whether received directly or through an anti-spamming organization, shall be presumed to be evidence that the message was unsolicited. Provider has no obligation to forward the complaint to the user or to identify the complaining parties.

10. User is responsible for the use of all Services utilized via its connection to the Provider network, including any support services provided via its connection to the Provider network. Support services includes, without limitation, hosting websites, electronic mailboxes, telephony gateways, IRC servers, advertising, transmitting, or otherwise making available any software, program, product or service that is designed to violate this AUP or the AUP of any other internet services provider. Conduct that directly or indirectly encourages, permits or relies on activities in violation of this AUP, is also a violation of the AUP. Examples include, without limitation, failure to implement technical or administrative measures to prevent mass unsolicited e-mail, or providing Spamming support services such as email drop boxes, sales of spamware, list washing, and the hosting of "spam-vertised" websites.

11. Nothing contained in this policy shall be construed to limit Provider's actions or remedies in any way with respect to any of the foregoing activities, and Provider reserves the right to take any and all additional actions it may deem appropriate with respect to such activities, including without limitation taking action to recover the costs and expenses of identifying offenders and removing them from the Provider service, and levying cancellation charges to cover Provider's costs. Provider will investigate violations of policy and will cooperate with law enforcement officials for suspected criminal violations. In addition, Provider reserves at all times all rights and remedies available to it with respect to such activities at law or in equity.

12. FILTERING SOFTWARE TO PROTECT MINORS

Pursuant to 47 U.S.C. Section 230(d) as amended, Provider notifies Users that parental control protections (such as computer hardware, software, or filtering services) are available that may assist Users in limiting access to material that is harmful to minors. Information identifying current providers of such protections is available at the America Links Up website, <http://penta2.ufrgs.br/gereseg/censura/netpar/parent.htm>.

Provider's Services include and permit access to many areas of the Internet, including sites that maintain discussions or content intended for adult audiences. Users represent that they are at least eighteen (18) years of age and assume all liability associated with viewing content or exposing any minor or other person to content in the Internet.