



ASPIRA's Communications and Computer Technology Acceptable Use Policy

Introduction

This Acceptable Use Policy ("AUP") sets forth the principles that govern the use by customers of the communications and computer technology systems, services and products provided by ASPIRA National Office (herein called "ASPIRA" or "the Organization"). The AUP has been created to promote the integrity, security, reliability and privacy of ASPIRA's systems and networks.

Compliance With Law

Customers shall not post, transmit, re-transmit or store material on or through any of Organization's system services or products that: (i) is in violation of any local, state, federal or non-United States law or regulation; (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons"); or (iii) violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ASPIRA.

Prohibited Uses of Organization's Systems, Services and Products

This AUP identifies the actions that the Organization considers to be abusive, and thus, strictly prohibited. In addition to the other requirements of this AUP, Customer may only use the Organization's systems, services and products in a manner that, in the Organization's sole judgement, is consistent with the purposes of such systems, services and products. If a customer is unsure whether a contemplated use or action is permitted under the AUP, the customer should

e-mail Organization with a description of the proposed use at jvillamil@aspira.org for a determination as to whether the use is permissible under this AUP. The examples identified in the subsections below are non-exclusive and are provided, in part, for guidance purposes.

The following uses of the Organization's systems, services and products as described in subsections A through E are expressly prohibited:

A. Prohibited Actions: General Conduct

1. Transmitting on or through any of Organization's systems, services, or products any material that is, in Organization's sole discretion, unlawful, obscene, threatening, abusive, libelous, or hateful, or encourages conduct that may constitute a criminal offense, may give rise to civil liability, or otherwise may violate any local, state, national or international law.
2. Transmission, distribution, or storage of any information, data or material in violation of United States or state regulations or law, or by the common law.
3. Violations of the rights of any Person protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.
4. Actions that restrict or inhibit any Person, whether a customer of the Organization or otherwise, in its use of any of the Organization's systems, services or products.
5. Resale of the Organization's services and products, without the prior written consent of Organization.
6. Use, installation, distribution, or duplication of any unauthorized software.

B. Prohibited Actions: System and Network Security

1. Attempting to circumvent user authentication or security of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for the customer, logging into a server or account the customer is not expressly authorized to access, or probing the security of other networks (such as running a SATAN scan or similar tool).
2. Effecting security breaches or disruptions of Internet communications. Security breaches include, but are not limited to, accessing data of which customer is not an intended recipient or logging onto a server or account that customer is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, and attempts to "crash" a host.
3. Using any program/script/command, or sending messages of any kind, designed to interfere with a user's terminal session, by any means, locally or by the Internet.

4. Executing any form of network monitoring which will intercept data not intended for Customer.

C. Prohibited Actions: E-Mail

1. Harassment, whether through language, frequency, or size of messages, is prohibited.
2. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material ("e-mail spam"). Customers are explicitly prohibited from sending unsolicited bulk mail messages. This includes, but is not limited to, bulk-mailing of commercial advertising, informational announcements, and political tracts. Such material may only be sent to those who have explicitly requested it. If a recipient asks to stop receiving e-mail, the Customer must not send that person any further e-mail.
3. Creating or forwarding "chain letters" or other "pyramid schemes" of any type, whether or not the recipient wishes to receive such mailings.
4. Malicious e-mail, including, but not limited to, "mailbombing" (flooding a user or site with very large or numerous pieces of e-mail).
5. Unauthorized use, or forging, or mail header information.
6. Using a Organization or a customer account to collect replies to messages sent from another provider.
7. Use of unsolicited e-mail originating from the ASPIRA network or networks of other Internet Service Providers on behalf of, or to advertise any service hosted by ASPIRA, or connected via the ASPIRA network.
8. Willful failure to secure open SMTP ports so as to prevent the unauthorized use of customer resources for the purposes of sending unsolicited e-mail by a third party.

D. Prohibited Actions: Usenet Newsgroups

1. Positing the same or similar messages to large numbers of Usenet newsgroup ("Newsgroup spams or USENET spam").
2. Posting chain letters of any type.
3. Posting encoded binary files to newsgroups not specifically named for that purpose.
4. Cancellation or superseding of posts other than your own, with the exception of official newsgroup moderators performing their duties.
5. Forging of header information. This includes attempting to circumvent the

approval process for posting to a moderated newsgroup.

6. Solicitations of mail for any other e-mail address other than that of the poster's account or service, with intent to harass or to collect replies.
7. Postings that are in violation of the written charters or FAQ's for those newsgroups.
8. Posting of Usenet articles from the ASPIRA network or networks of other Internet Service Providers on behalf of, or to advertise any service hosted by ASPIRA, or connected via the ASPIRA network.
9. Failure to secure a news server so as to prevent the unauthorized use of customer resources by a third party which may result in Usenet posts which violate this policy.
10. Advertisements posted in newsgroups whose charters/FAQ's explicitly prohibit them. The poster of an advertisement or other information is responsible for determining the etiquette of a given newsgroup, prior to posting to it.

E. **Prohibited Actions: Individual Accounts (Dial-up Users Only)**

1. Utilizing multiple logins, except as allowed by the Organization-provided version of 'screen'. Users of 'user mode IP' programs (such as TIA) may use one additional login via telnet in addition to the initial login. Shell account users may not run programs that provide network services from their accounts, such as IRC or MUD servers.
2. Attempting to circumvent the 'idle daemon' or time charges accounting, or attempts to run programs while not logged in by any method, are prohibited.
3. Consuming excessive resources, including CPU time, memory, disk space, and session time. The use of resource-intensive programs which negatively impact other system users or the performance of Organization systems or networks is prohibited, and Organization staff may take action to limit or terminate such programs.
4. Sharing of passwords or accounts with others.

Complaint and Enforcement

A. **Complaint**

Complaints regarding abusive conduct may be reported to:

Ronald Blackburn-Moreno
ASPIRA National Office
1444 I Street, NW Suite 800

ASPIRA must be able to independently verify each instance of abuse, and so each complaint must include the COMPLETE TEXT OF THE OBJECTIONAL MESSAGE, INCLUDING ALL HEADERS. Please do NOT send excerpted parts of a message; sending a copy of the entire message, including headers, helps to prevent misunderstandings based on incomplete information, or information used out of context. Full headers demonstrate which path the message has taken, and enable us to determine whether any part of the message has been forged. This information is vital to our investigation.

B. Enforcement

The Organization may suspend, terminate, or otherwise limit a user's access to services for violations of the AUP without warning. In practice warnings and corrective action will be attempted before administrative actions are taken. All infractions to the AUP will be reported to management for administrative review and may effect your employment record. Specific administrative actions are not specified within this document.

Miscellaneous

A. Modification of AUP

Organization retains the right to modify the AUP at any time and any such modification shall be automatically effective as to all customers when adopted by Organization.

B. Applicability of AUP

The actions listed herein are also not permitted from other Internet Service Providers. Deceptive marketing, as defined by the Federal Trade commission Deception Policy Statement, is not permitted through the ASPIRA services or network. These rules apply to other types of Internet-based distribution mediums as well, such as RLG's Ariel system (a system for sending FAX-like documents over the Internet).

C. Organization Is Not Responsible For Content

Organization is not responsible for the content of any USENET posting, whether or not the posting was made by a customer of the Organization.

D. Removal of Materials

At its sole discretion, Organization reserves the right to remove materials from its servers and to terminate internet access to customers that Organization determines have violated this AUP.

This AUP was approved and adopted by the ASPIRA National Board of Directors on:
