AUP (ACCEPTABLE USAGE POLICY)

ACCEPTABLE USE POLICY (AUP)

This Acceptable Use Policy (AUP) is intended to help protect Trust Systems customers, and the Internet community, from the inappropriate use of the Internet. A customer's use of Trust Systems service constitutes acceptance of this AUP. Trust Systems reserves the right to revise and update this AUP from time to time. Trust Systems expects customers to cooperate with the company's Abuse department when requested to assist in their investigations.

THIS AUP IS DIVIDED INTO TWO PARTS:

Part 1. Violations and Descriptions of Appropriate Use
Part 2. Reporting to Trust Systems TOS/Abuse department

PART 1: VIOLATIONS AND DESCRIPTIONS OF ACCEPTABLE USE 1.1 GENERAL VIOLATIONS

Our AUP prohibits the following:

Impersonation/Forgery - Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers and nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed provided appropriate contact information is contained in the body of the posting.

Privacy Violations - Attempts, whether successful or unsuccessful, to gain access to any electronic systems, networks or data, without proper consent, are prohibited.

Threats - Threats of bodily harm or destruction of property are prohibited.

Harassment - Threatening or harassing activity is prohibited.

Illegal Use - The use of any Trust Systems service for illegal purposes is prohibited.

Reselling - The resale of any Trust Systems service without proper authorisation from Trust Systems Ltd. is prohibited. Persons wishing to act as resellers may contact us to obtain details of our wholesale partner.

Copyright Infringement - All material published must be owned by the publisher or the appropriate releases must have been obtained prior to publishing. Trust Systems will co-operate with all agencies attempting to assert their rights in these matters.

1.2 NETWORK DISRUPTIONS AND NETWORK-UNFRIENDLY ACTIVITY

Any activities, which adversely affect the ability of other people or systems to use Trust Systems services or the Internet, are prohibited. This includes "denial of service" (DoS) attacks against another network host or individual user. Interference with, or disruption of, use of the network by others, network services or network equipment is prohibited. It is the customer's responsibility to ensure that their network is configured in a secure manner. A customer may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A customer may not permit their network, through action or inaction, to be configured in such a way that it gives a third party the capability to use their network in an illegal or inappropriate manner.

1.3 E-MAIL

Trust Systems does not tolerate, endorse or participate in e-mail spamming. Sending unsolicited commercial e-mail is prohibited. We cannot authorise bulk emailing although

we do recognise that in some instances this is a valid and useful form of marketing for both

1.6 WEB

Using a Trust Systems Web site address or Trust Systems hosted Web account for the purpose of distributing illegal material is prohibited. Trust Systems will co-operate with authorities to remedy breaches of this policy.

Using a Trust Systems Web site address or Trust Systems hosted Web account to collect responses from unsolicited commercial e-mail is also prohibited.

1.7 EXCESSIVE BANDWIDTH OR DISK UTILISATION

Trust Systems account descriptions specify current limits on bandwidth and disk utilisation. Where limits are not specifically defined the judgement of the Trust Systems Technical Support team shall be used to define those limits. The use of bandwidth or disk space in excess of those limits is not permitted. The total number of bytes transferred from an account's Web and FTP space determines bandwidth utilisation. The total number of bytes required to store an account's Web, FTP, and Mail data determines disk utilisation. If Trust Systems determines that excessive bandwidth or disk space utilisation is adversely affecting Trust Systems' ability to provide service, Trust Systems may take immediate action. Trust Systems will attempt to notify the account owner by e-mail as soon as possible.

2. REPORTING TO TRUST SYSTEMS'S ABUSE DEPARTMENT

Trust Systems requests that anyone who believes that there is a violation of this AUP should direct the information to the AUP Abuse Staff at this address: support@trustsystems.co.uk Trust Systems customers who wish to report 'spam' from a non-Trust Systems source should send copies of the e-mail they received along with full header information. Some messages may not receive a response, but Trust Systems may use the information received at this address to aid in the development of Trust Systems' filter lists. All issues involving other e-mail abuse originating from Trust Systems e-mail or network addresses should also be sent to the above address, along with all issues regarding USENET 'news' abuse issues originating from Trust Systems customers, other suspicious activity such as port scans or attempts to penetrate network resources and virus distribution and copyright infringement.

TRUST SYSTEMS MAY TAKE ANY ONE OR MORE OF THE FOLLOWING ACTIONS IN RESPONSE TO COMPLAINTS:

- Issue warnings: written or verbal
- Suspend the customer's newsgroup posting privileges
- Suspend the customer's account
- Terminate the customer's account
- Invoice the customer for administrative costs, loss of service and/or reactivation charges

WHAT INFORMATION SHOULD BE SUBMITTED?

- The IP address used to commit the alleged violation
- The date and time of the alleged violation, including the time zone or offset from GMT
- Evidence of the alleged violation Copies of e-mail with full header information provide all the required information, as do syslog files and firewall logs. Other situations will require different methods.