Acceptable Use Policy

General

Use of Reliable's Software or Hosting Services for illegal activities of any kind, including unauthorized use (or attempted unauthorized use) of Reliable's network or equipment or unauthorized use of other networks or equipment on the Internet or other Reliable customer networks, forging header information or user identification information, spoofing IP address information and software piracy is prohibited.

Network Use

Reliable maintains its network for the joint use of its customers and other stakeholders. Any activity which is deemed by Reliable to disrupt the normal functioning of network, components, servers or other facilities shall be a violation of this AUP. This includes but is not limited to:

- Sending of traffic which serves no legitimate purpose.
- Generating random network traffic.
- Sending traffic to or from RFC1918 addresses over the public Internet.
- Spoofing the source address of any IP or Ethernet packet.
- Sending traffic with the intent to deny service to any other party.
- Hosting services or materials that generate too much traffic to or from the Internet.
- Hosting materials or services that attract miscreants.
- Port scanning of any computer or network.
- Attempting unauthorized access to any computer or network device including devices outside the Reliable Hosted Service.
- Hosting or transmitting copyrighted works without authorization.

E-mail

Sending harassing or mass unsolicited e-mail is prohibited. Forging header information in e-mail is prohibited. Use of programs such as mflash or storage of such programs on Reliable's servers is prohibited. Reliable maintains a zero tolerance to Unsolicited Commercial Email and Network Abuse. Running a server or workstation which provides an Open Relay or Open Proxy, which allows others to send unsolicited commercial e-mail, or transmit viruses or internet worms is strictly prohibited.

Reliable's email relay servers are for sending personal or business email using common Internet email software such as Microsoft Outlook, Thunderbird, Eudora Mail, and other end-user email clients. The servers may not be used to send bulk email, whether solicited or

unsolicited, at any time. In addition, Reliable customers who operate their own mail server software shall configure that software to send mail directly to the Internet, and not relay through Reliable servers as a 'smart host'.

Reliable does not permit the use of network facilities or routed IP addresses for sending of unsolicited email of any kind, for any purpose whatsoever. A Reliable customer shall be responsible to secure access to Reliable facilities and network from intrusion by third parties. The Customer shall be responsible for any violation of this AUP which originates from a circuit under the Customer's control, whether known or unknown to the Customer.

The following is a list of specific examples of activities which constitute a violation of this AUP with respect to email. This is not an exhaustive list but is representative of common violations which have been observed from Customer circuits.

- Allowing the connection of a computer infected with a "Bot" or other software under the control of a third party used for nefarious purposes such as sending mass email, port scanning, dictionary attacks, DOS attacks, or the spread of computer viruses or "Bots" to a Reliable's circuit or network.

- Relaying of mass mailings of any type through Reliable email servers. Any mailings of a quantity sufficient to disrupt normal customer usage of Reliable email servers by other customers shall be a violation.

- Sending email to non-existent email addresses. Email which cannot be delivered and uses the resources of Reliable email servers to the extent that normal usage by other Customers is disrupted shall be a violation.

- Sending of email which generates complaints from recipients. This includes emails of any nature which are unwanted by the recipient.

- Sending of email for the purpose of gaining personal or other information from the recipient through fraud. These "phishing" emails may also constitute a violation of law. Hosting a website for these purposes is also a violation.

- Forging or using an email address other than your own in the envelope sender or From: field of any email. Using email as a means to misrepresent one's identity to the recipient.

- Violating another provider's rules regarding acceptance of bulk email. It shall be the customer's responsibility to abide by policies of other networks with regard to accepting bulk email which is solicited by the recipient. Complaints received by Reliable which show violation of other provider's policies shall be a violation of this AUP.

World Wide Web

Use of web pages for advertising purposes requires a Reliable Business Account. Reselling web space, selling advertising on a web site, or taking credit card orders requires a Reliable Commercial Account. Pages containing pornography or nude images may not be stored on Reliable's web servers. Any other adult-oriented material should have warning and disclaimer pages, if not password protection. Use of text or images created by others

without their permission is copyright infringement and is prohibited. Reliable reserves the right to shut down any site due to excessive use.

Public FTP Sites

Use of Reliable's FTP server for advertising purposes requires a Reliable business account. Reselling FTP space is prohibited. Files containing pornography or nude images may not be stored on Reliable's FTP server. Using Reliable's FTP server for the exchange of pirated software or software designed to facilitate copyright infringement, unauthorized use of computer systems, credit card fraud, or other illegal activity is prohibited.