ACCEPTABLE USE POLICY

This acceptable use policy defines COLO@ 's policy designed to protect COLO@ and persons and entities using COLO@ products and services, including Internet service (collectively, "customers") from negative impact caused by inappropriate activities. COLO@ reserves the right to modify this policy from time to time. Customers shall adhere to this policy and are subject to the terms and conditions herein. Each customer's use of COLO@ 's products and/or services constitutes acceptance of the Acceptable Use Policy in effect at the time of use. If at any time a customer elects not to accept this policy, the customer shall discontinue use of COLO@ 's products and/or services.

Acceptable Use

Each customer is responsible for ensuring that its access to and management activities on its systems, data and content does not impose risks to or negative impacts on COLO@ or other sites or systems. Each customer is also responsible for any misuse of accounts on its systems located at COLO@ . Each customer shall adhere to all local, state, federal and international laws and regulations regulating customer operations.

Unacceptable Uses

Each customer is responsible for ensuring that it does not knowingly allow its systems hosted by COLO@ to be used for any of the following:

(1) posting, transmission, re-transmission, or storing material on or through any of COLO@ 's products or services, if in the commercially reasonable judgment of COLO@ such posting, transmission, re-transmission or storage is: (a) in violation of any local, state, federal, or international law or regulation; (b) harassing (through language, frequency or size of message); (c) obscene; (d) hateful; or (e) libelous.

(2) installing or distributing "pirated" or other software products that are not licensed for use by customer.

(3) deceptive marketing practices.

(4) actions that restrict or inhibit COLO@ 's or its customers' use or enjoyment of COLO@ 's products and services, or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or business use of Internet services.

(5) introducing malicious programs (e.g., viruses, trojan horses and worms) into the COLO@ network or servers or other products and services of COLO@ .

(6) causing or attempting to cause security breaches or disruptions of Internet communications. Examples of security breaches include but are not limited to accessing data of which the customer is not an intended recipient, or logging into a server or account that the customer is not expressly authorized to access. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information. This also includes no IRC on the network.

(7) executing any form of network monitoring that will intercept data not intended for the customer.

(8) circumventing user authentication or security of any host, network or account in any way, including, but not limited to: (a) configuring systems to bypass security controls; (b) conducting online security audits or tests against or through COLO@ systems or networks without coordination with and the explicit written consent of an authorized manager of COLO@ ; (c) installation of programs or configuring systems to allow "sniffing" of data traveling over a shared network; (d) installing or using software for the purposes of cracking encrypted data including, without limitation, stored passwords; and (e) removing or disabling security software or services including, without limitation anti-virus software, logging utilities or authentication services.

(9) interfering with or denying service to any user other than the customer's host (e.g., denial of service attack).

(10) using any program/script/command, or sending messages of any kind, designed to interfere with, or to disable a user's terminal session.

(11) furnishing false or incorrect data on the order form contract (electronic or paper) including fraudulent use of credit card numbers or attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization or other methods to document "use" of COLO@ 's products or services.

(12) sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers of the customer or with whom the customer does not have an existing business relationship (e.g., e-mail "spam").

(13) solicitations of mail or any other E-mail address other than that of the poster's account or service, with the intent to harass or collect replies.

(14) creating or forwarding "chain letters" or other "pyramid schemes" of any type.

(15) use of unsolicited E-mail originating from within the COLO@ network or networks of other Internet service providers on behalf of or to advertise any service hosted by COLO@ or connected via the COLO@ network.

(16) exporting, re-exporting, or permitting downloads of any content in violation of the export or import laws of the United States or without all required approvals, licenses and exemptions.

(17) high yield investment programs.

(18) sites that are attacking in nature - specifically "sucks" types sites and sites that use others corporate names to promote them as sucking or use their corporate image / logo exactly or in slightly altered ways are expressly disallowed.

(19) altering, defacing or otherwise causing any unauthorized or unapproved modification of any system belonging to COLO@ , another customer or any other system on the Internet;

(20) violating the privacy rights of others, including, without limitation, the collection of information about individuals without their knowledge or consent, except as allowed by applicable laws and regulations;

(21) engaging in, or permitting, any activity that leads to a degradation or denial of service for COLO@ , another customer or any other system or site on the Internet;

(22) violating the rules or policies of any other hosting provider, message service, chat room, bulletin board, newsgroup or similar system, service or provider;

(23) intentionally, recklessly or negligently omitting, forging, deleting or misrepresenting transmission information—including, without limitation, headers, return-address information and IP addresses—that is intended to cloak or hide the identity or source of information transmitted by the customer's systems, customers or users; or

Enforcement

Each customer shall implement measures and procedures to ensure that its systems are not accessed or used in an unauthorized manner, including, without limitation, the following: (1) maintaining, and providing COLO@ with, a list of authorized individuals and accounts that are permitted to remotely access such customer's systems hosted by COLO@ ; (2) notifying COLO@ in writing if a user no longer requires remote access to such customer's site (COLO@ must receive this notification at least five business days in advance of the date that the access is no longer needed); (3) remote-access accounts shall not be transferred from one individual to another, nor shall they be shared between individuals. Upon notification of a violation, customers shall immediately take all commercially reasonable and necessary steps to avoid any further abuse of such resource.

COLO@ may be notified of a violation in a number of ways, including by an external organization, agency, entity or individual that is affected by the activities of a customer or, when a violation is detected internally, by a source within COLO@ . COLO@ retains the sole right to determine whether a violation of this policy has occurred. Generally, COLO@ will attempt to work with a customer to address violations of this policy, but COLO@ is not required to do so. Based on the severity of the violation or the number or nature of complaints received, COLO@ , in its sole discretion, has the absolute right to immediately terminate service; provided, however, that COLO@ will use commercially reasonable efforts to notify Customer prior to or upon such suspension. COLO@ has the right to seek legal remedies for any damages, costs or expenses that may be incurred as a result of a violation of any of this policy by or through a customer.

If COLO@ believes that systems located within COLO@ facilities are being used in an unlawful or improper manner or for unlawful or improper activities, COLO@ will fully cooperate with civil and/or criminal enforcement authorities conducting investigations of such use or activities. COLO@ will also support the investigation of the unacceptable uses listed above and any other activities that COLO@ , in its sole discretion, believes adversely impact the operation or security of COLO@ , customers or other systems accessible by customers or customers' clients or users.

No failure or delay in enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in law, such provision shall be disregarded and the balance of the policy shall remain in effect.

Electronic Communications Privacy Act Notice

COLO@ makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon COLO@ technology, and makes no guarantee that any other entity or group of users will be included or excluded from COLO@ 's network. COLO@ may periodically monitor transmissions over its network for maintenance, service quality assurance or any other purpose permitted by the Electronic Communications Privacy Act, P.L. No. 99-508, as amended.