Updated January 2016

cologix

Hosting and Managed Services Acceptable Use Policy

Key Comment	**Who Should Read this?**
This policy provides Cologix customers ordering hosting and managed services from Cologix with standards and rules regarding their use of such services.	*All Cologix customers ordering hosting and managed services.*

This Hosting and Managed Services Acceptable Use Policy (this "Policy") defines acceptable practices relating to the use of Cologix's dedicated and cloud managed services (each, a "Managed Service" and, collectively, "Managed Services") by customers ("Customers") of Cologix, Inc. and each of its affiliates ("Cologix") and by users that have gained access to a Service through a Customer's account ("Users"). By using a Service, you acknowledge that you and your Users are responsible for compliance with this Policy. You are responsible for violations of this Policy by any User that accesses a Service through your account, which includes, without limitation, Users for whom you provide services as a reseller of Cologix's Managed Services. As used herein, "you" refers to Customers, and any reference to "Users" is intended to encompass, as applicable, both Customers and their Users. As used herein, "Managed Services" shall include, without limitation, all equipment, systems, software, services, and products incorporated or used in hosted computer and storage services.

This Policy is designed to assist in protecting the Cologix network, the Managed Services, Cologix customers and the Internet community as a whole from improper and/or illegal activity, to improve Managed Services and to improve network services offerings. In situations where data communications are carried across networks of other Internet Service Providers ("ISPs"), Users of the Cologix network must also conform to the applicable acceptable use policies of such other ISPs.

CUSTOMER CONSENT TO POLICY

Use of Managed Services

1. Customer agrees to use Cologix's Managed Services for lawful purposes, in compliance with all applicable laws.

2. Cologix dial-up accounts are provided for use in conformance with this Policy. Cologix reserves the right to investigate suspected violations of this Policy. When Cologix becomes aware of possible violations, Cologix may initiate an investigation, which may include gathering information from the Customer or Customers involved and the complaining party, if any, and examination of material on Cologix's servers.

3. During an investigation, Cologix may suspend the account or accounts involved and/or remove the material involved from its servers, and Cologix is not responsible in any way for any damages resulting therefrom. If Cologix believes a violation of these rules has

occurred, it may take responsive action at its sole discretion. Such action may include, but is not limited to, temporary or permanent removal of material from Cologix's servers, the cancellation of news group posts, warnings to the Customer or Customers responsible, and the suspension or termination of the account or accounts responsible. Cologix, at its sole discretion, will determine what action will be taken in response to a violation on a case-by-case basis. Violations of these rules could also subject Customer to criminal or civil liability.

Use of Materials

1. Materials in the public domain (e.g., images, text, and programs) may be downloaded or uploaded using Cologix's Managed Services. Customers may also re-distribute materials in the public domain. Customer assumes all risks regarding the determination of whether material is in the public domain.

2. Customer is prohibited from storing, distributing or transmitting any unlawful material through Cologix's Managed Services. Examples of unlawful material include, but are not limited to, direct threats of physical harm, child pornography, and copyrighted, trademarked and other proprietary material used without proper authorization. Customer may not post, upload or otherwise distribute copyrighted material on Cologix's servers without the consent of the copyright holder. The storage, distribution, or transmission of unlawful materials could subject the Customer to criminal as well as civil liability, in addition to the actions outlined in the "USE OF MANAGED SERVICES" section above.

3. Customer may not store or distribute certain other types of material on Cologix's servers. Examples of prohibited material include, but are not limited to, programs containing viruses or trojans and tools to compromise the security of other sites.

Passwords

1. Cologix personal dial-up accounts are for individual use only. Customers may not share passwords or accounts with other individuals.

2. In the event that the security of a Customer is compromised, Cologix may require the Customer to use a new password.

3. Cologix staff may check the security of a Customer's passwords at any time. A Customer with an insecure password may be asked to change the password to one which complies with the above rules. Customers who repeatedly choose insecure passwords may be assigned a password by Cologix. Continued failure to maintain password security may be grounds for account termination.

System Security

1. Customer is prohibited from utilizing Cologix Managed Services to compromise the security of, or tamper with, Cologix's system resources or accounts on any of Cologix's computers, routers, terminal servers, modems, or any other equipment at Cologix or at any other site. Use or distribution of tools designed for compromising security is prohibited. Examples of the tools include, but are not limited to, password guessing

programs, cracking tools or network probing tools. Any attempt to access any of Cologix's corporate assets is strictly prohibited.

2. Cologix reserves the right to release the user names of Customers involved in violation of system security to system administrators at other sites, in order to assist them in resolving security incidents. Cologix will also fully cooperate with law enforcement authorities in investigating suspected lawbreakers.

System Resources

1. Cologix will allocate system resources to provide all Customers with the best service possible. As part of resource allocation, Cologix may limit, restrict or prioritize access to system resources, including CPU time, memory, disk space, session length, and number of sessions.

2. Additionally, Cologix may institute services and fees for Customers who are interested in accessing system resources above and beyond acceptable usage. See the "ACCEPTABLE USAGE" section below.

3. Cologix may log instances of abuse of system resources, including but not limited to those outlined below, and take action as outlined in the "USE OF MANAGED SERVICES" section above.

4. System abuse is defined as any use of Cologix resources which disrupts the normal use of system or Internet services for others. Examples of system abuse include, but are not limited to, attempting to disrupt the sessions of other Internet users, consuming excessive amounts of memory, disk space, or bandwidth, or otherwise affecting the performance of Cologix's servers or networks.

5. Customers may not run programs which provide network services from their accounts. Example of prohibited programs include, but are not limited to, mail, http and irc servers, and multi-user interactive forums.

6. Customers may only make use of Cologix system resources while logged in. The sole exceptions to this policy are email filters, which process and sort mail as it arrives.

ACCEPTABLE USAGE

Acceptable usage is hereby defined as the normal activities associated with the usage of the Internet, including, but not limited to, usage of Cologix's systems and network facilities for accessing the WWW, IRC, Usenet News, E-Mail, and other Internet features. Depending on the account type, this may include file storage on Cologix's servers for Customer's own personal web page, file access area (FTP), and possibly Unix utilities used in a shell account. Shell users may be permitted to use their own software on Cologix's servers, subject to Cologix's examination and approval, provided such software does not use excessive system resources or in any way compromise system integrity and does not fall under any of the prohibited activities listed within this document.

This Policy is subject to any and all laws and regulations set forth by the Federal, State or any other governmental authority.

PROHIBITED ACTIVITIES

Activities specifically prohibited by Cologix include, but are not limited to, the following:

1. Background and/or server-type applications. Including but not limited to IRC bots, HTTP servers, MUDs, and any other process which were initiated by the user that continues execution on the system upon user logout.

2. Long-term storage of data. Long-term storage of data is referred to as the storage of files which are not used regularly in an account for an extended period of time. This specifically includes but is not limited to programs such as shareware programs which the user may download to their account for purposes of transferring to their home computer. Such programs should be removed at such time as they are successfully transferred to the user's personal system.

3. Flooding or abuse of other users. Flooding is a fairly common occurrence on the Internet, and one which is dealt with strictly at Cologix. Flooding takes place in numerous ways, including but not limited to ICMP flooding, mail bombing (sending large amounts of e-mail repeatedly to a person for purposes of harassment), mass mailings to multiple addressees, msg/CTCP flooding on IRC, as well as other, less common methods.

4. Attempts to compromise system and/or network security. Programs such as packet sniffers, password crack programs, and similar utilities found to be running from a user's account are prohibited. This also includes attempts to hack into non-Cologix systems.

5. Sharing of accounts. Sharing of a user's account with another party for purposes of avoiding payment for a second account is strictly prohibited.

6. Attempts to bypass resource usage limitations. In order to provide fair service to all Cologix users, Cologix has implemented certain resource limitations, the two most common being disk quotas on the servers, and idle time-outs on dial-ups. Attempts to bypass disk usage quotas by any means may result in immediate loss of system privileges. Attempts to bypass the idle time-outs are also prohibited. The current idle time-out limit is twenty minutes.

7. PPP/SLIP Emulation software. Since PPP/SLIP is a product offered by Cologix, users desiring such access are required to sign up for that service rather than attempting to emulate it by software. Any such software will be removed from the user's account by Cologix immediately when found. All software provided by Cologix to Customers is copyrighted by Cologix and may not be tampered with, decompiled or reverse engineered.

8. Excessive use of system resources. This segment can be broken down into two different parts, system and dial-up. For system purposes, this can be defined as the continued use of programs or commands which take a large amount of system resources, be that

processor time, network bandwidth, and/or drive space on the host system. For dial-up purposes, this primarily prohibits the continued usage of a dial-up port to simulate a dedicated connection for the user's home system. Dial-up accounts are designed to provide on-demand access for Customers, not dedicated connections. If a dedicated connection is desired, the Customer needs to speak with its Cologix sales account representative.

9. E-mail Abuse. E-mail abuse typically comes in one of three forms, the transfer of an unsolicited message to individuals (spamming), the sending of harassing and/or threatening messages to other users, and the forging of e-mail addresses so as to make the e-mail appear to be from another user.

10. Usenet order News Abuse. Similar to e-mail abuse, includes forging of addresses, harassment/threats, the posting of the same message to multiple news groups (spamming), as well as the posting of information in groups where it is not relevant and unwanted.

11. Pyramid/Money-Making schemes (MMF, or Make Money Fast Scams). Such activities as the transfer of information or solicitation of persons via the Internet in an attempt to extort money or other valuables or the use of pyramid/chain letters are all illegal, and all prohibited.

12. Pirated Software. Pirated software is defined as the illegal exchange of software via the Internet for purposes of avoiding the purchase of said software by the individuals involved. This includes most commercial applications such as Adobe Photoshop, Illustrator, etc. Such activities are prohibited by Federal law and are thus not allowed in any form on Cologix. Such prohibition also includes the unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources and copyrighted software. The exportation of software or technical information in violation of U.S. export control laws is strictly prohibited.

13. High-Traffic Web sites. Individual accounts on Cologix machines are intended to provide access to individuals only. As most individual pages are fairly low-traffic for the most part, the performance for everybody on the systems is optimal. However, some individuals occasionally choose to put content on their pages which draws a large number of hits to their pages and thus degrade performance for other users' pages. Due to this, Cologix has had to implement certain limitations on the amount of traffic an individual user's home page can receive. Typically a page can safely receive around 4-5,000 hits per day and/or transfer under 20-25 megs per day without causing excessive load on the host system. Sites generating more than this must be moved over to Cologix's Web Hosting services, which are better suited to deal with the extra traffic.

PENALTIES FOR ABUSE

1. Penalties for account abuse include termination of a user's account and any applicable legal penalties. The penalties imposed on a user for abuse will vary based on the level of the offense. Cologix will usually give a warning on the first offense, but will terminate the account immediately and without warning if the offense is severe enough. Accounts closed due to Customer abuse will not be reopened.

It is vital for Cologix to provide a quality service for all users, and Cologix will not tolerate users who through their actions hinder us in that endeavor. It is also important for Cologix to have a non-intrusive presence to the rest of the Internet, and thus prohibited activities which adversely affect users on other service providers and their associated networks. To this end, Cologix reserves the right to modify and/or disable user service at any such time abuse occurs.

2. Cologix will not reimburse users whose service was suspended or disabled due to any of the reasons listed above.