Webnet International Company
Plot 110 Bukoto Street, Kamwokya
P.O.Box 34112, Kampala Uganda

Phone Numbers: +256772975207,
+256- 312105068, +256-414595955

Emails:sales@webnet.co.ug
Url:http://www.webnet.co.ug

Webnet's Acceptable Use Policy ("AUP")

General Statement

Webnet is dedicated to the unrestricted free transmission of information via the internet and its many resources. Our goal is to deliver enterprise quality on-demand IT services to all of our Customers while serving as the medium of exchange for transmission of all information. The storage, distribution, and exchange of information (content) are the internet's single most valuable feature. Webnet is dedicated to protecting the source and distribution of information and protecting the rights and privileges of those utilizing it. Webnet does not purport to be the content police; our duty in the process of information dissemination is simply to act as conduit between interested parties. Webnet follows all local, state and federal laws pursuant to the services delivered over the internet and directly related to our network and internal systems. The purpose of this AUP is to inform all Customers of acceptable, anticipated Customer use. Due to the myriad of possibilities in maintaining a network comprised of thousands of servers, this AUP is intended to act as a guideline to service and not to be all encompassing.

Public Network

The primary purpose of the Webnet Public Network is to transmit information (packets) to and from Customer servers and data storage services. Proper use of the Public Network is to utilize the network in any way so long as Customer does not violate any local, state, or federal laws or generate harm to the network or interfere with the use of services of other users utilizing the same network. All Customers are granted equal access to the Public Network. Violation, misuse, or interference of the public network shall be considered a violation of the AUP and shall trigger the Methods of Resolution under this AUP as set forth below in Table C.

Private Network

The primary purpose of the Webnet Private Network is to allow secure private network connectivity to the private backend network directly connecting Customer servers and Webnet delivered services. Proper use of the Private Network is the upload/download of content, server administration, transmission of information between servers, transmission of information between servers and Webnet servers, secure private administration of services, data retrieval, console access, and true out of band management of their entire IT environment. The Private Network can also be utilized for service access during periods of non-payment, copyright infringement, spam abuse, service interruption or other instances requiring server administration. All Customers are granted equal access to the private secure network to securely manage their services. Connectivity to the Private Network is granted on an unrestricted basis in eight (8) hour increments. Dedicated connections to the Private Network are available through the sales team. Violation, misuse, or interference of the Private Network shall be considered a violation of the AUP and shall trigger the Methods of Resolution under this AUP as set forth below in Table C.

Security Services

The primary purpose of the Webnet standard security services is to assist the Customer in the protection, management, update, and overall stability of the outsourced IT environment. Webnet also monitors all aggregate network traffic via Arbor networks and router netflow statistics for traffic analysis. Webnet also supplies Microsoft update servers and Red Hat update servers located on the Private Network for private secure update services. These services are included free of charge and are intended to assist Customers in the OS management of their servers. Other security services offered for a fee are covered via the terms of the individual services. These services include, but are not limited to: firewalls, host IDS, service monitors and other similar type products and services. Outside of the global network security services described above, Customers are required and obligated to maintain security related to Customer managed servers. The management of dedicated servers requires basic security management including password management, port management, OS updates, application updates, security policy settings and more. The Customer is ultimately responsible for individual server security unless contracted security services are purchased. Any violation of the security services included in basic services will be addressed pursuant to the Methods of Resolution under this AUP as set forth below in Table C.

Server Content

Webnet International Company
Plot 110 Bukoto Street, Kamwokya
P.O.Box 34112, Kampala Uganda

Phone Numbers: +256772975207,
+256- 312105068, +256-414595955

Emails:sales@webnet.co.ug
Url:http://www.webnet.co.ug

Webnet does not actively monitor dedicated server content for review. Webnet believes in the free dissemination of information via our services. Dedicated server content will only be reviewed upon complaint by verified third parties. Content that does not violate local, state and federal law or the AUP is deemed in compliance and shall remain intact. Legal adult content is allowed on Webnet dedicated servers. Content deemed in violation will be addressed pursuant to the Methods of Resolution under this AUP as set forth below in Table C.

Examples of unacceptable material on all Shared and Reseller servers include:

- Topsites
- IRC Scripts/Bots
- Proxy Scripts/Anonymizers
- Pirated Software/Warez
- Image Hosting Scripts (similar to Photobucket or Tinypic)
- AutoSurf/PTC/PTS/PPC sites
- IP Scanners
- Bruteforce Programs/Scripts/Applications
- Mail Bombers/Spam Scripts
- Banner-Ad services (commercial banner ad rotation)
- File Dump/Mirror Scripts (similar to rapidshare)
- Commercial Audio Streaming (more than one or two streams)
- Escrow/Bank Debentures
- High-Yield Interest Programs (HYIP) or Related Sites
- Investment Sites (FOREX, E-Gold Exchange, Second Life/Linden Exchange, Ponzi, MLM/Pyramid Scheme)
- Sale of any controlled substance without prior proof of appropriate permit(s)
- Prime Banks Programs
- Lottery/Gambling Sites
- MUDs/RPGs/PBBGs
- Hacker focused sites/archives/programs
- Sites promoting illegal activities
- Forums and/or websites that distribute or link to warez/pirated/illegal content
- Bank Debentures/Bank Debenture Trading Programs
- Fraudulent Sites (Including, but not limited to sites listed at aa419.org & escrow-fraud.com)
- Push button mail scripts
- Broadcast or Streaming of Live Sporting Events (UFC, NASCAR, FIFA, NFL, MLB, NBA, WWE, WWF, etc)
- Tell A Friend Scripts

Backups and Data Loss

Your use of this service is at your sole risk. Our backup service runs once a week, overwrites any of our previous backups made, and only one week of backups are kept. This service is provided to you as a courtesy. Webnet is not responsible for files and/or data residing on your account. You agree to take full responsibility for files and data transferred and to maintain all appropriate backup of files and data stored on Webnet servers.

Reseller: Client Responsibility

Resellers are responsible for supporting their clients. Webnet does not provide support to our Reseller's Clients. If a reseller's client contacts us, we reserve the right to place the client account on hold until the reseller can assume their responsibility for their client. All support requests must be made by the reseller on their clients' behalf for security purposes. Resellers are also responsible for all content stored or transmitted under their reseller account and the actions of their clients'. Webnet will hold any reseller responsible for any of their clients actions that violate the law or the terms of service.

Webnet International Company
Plot 110 Bukoto Street, Kamwokya
P.O.Box 34112, Kampala Uganda

Phone Numbers: +256772975207,
+256- 312105068, +256-414595955

Emails:sales@webnet.co.ug
Url:http://www.webnet.co.ug

DNS Services

Webnet supplies redundant domain names services for all Customers purchasing dedicated services. These services include the use of authoritative name servers for public resolution of domain names and private domain name resolvers located on the private service network. The DNS services are fully managed and maintained by Webnet with Customer specific domain name management through the online Customer portal. In rare instances, where extreme intensive loads (DNS lookups) utilize disproportionate resources of the redundant DNS systems, Webnet will notify Customer of potential violation of this AUP. Customers requiring such DNS services will be instructed to perform dedicated DNS services on Customer-managed equipment. Violation of DNS services shall trigger the Methods of Resolution under this AUP as set forth below in Table C.

IP Addresses

The IP Address Policy ("IP Policy"), which may be changed from time to time at Webnet's sole discretion, is incorporated into this MSA by reference and provides additional terms and conditions relating to IP Addresses. Customer acknowledges and agrees to adhere to the IP Policy. All Internet Protocol (IP) Addresses are owned and managed by Webnet. IP Addresses are non-transferable from Webnet, and Customer retains no ownership or transfer rights to IP Addresses. All IP Addresses are assigned by the Webnet engineering team on a per VLAN, per server basis. Attempted use of IP addresses not originally allocated for use or IP addresses use on non-assigned VLANs or servers is a violation of this AUP. Violation of the IP Address policy shall trigger the Methods of Resolution under this AUP as set forth below in Table C. Private IP assignments are available to qualified Customers.

IRC

Webnet allows the use of private Internet Relay Chat (IRC) servers for communication among private parties. Webnet absolutely prohibits the use of IRC servers connected to public IRC networks or servers. IRC servers that result in interference of service, malicious network activity or increased demand on network security services are in direct violation of this AUP. Violation of the IRC policy shall trigger the Methods of Resolution under this AUP as set forth below in Table C.

Peer to Peer

Webnet allows the use of internet Peer-to-Peer software for file sharing purposes. Webnet highly recommends strict oversight and management of Peer-to-Peer software environments due to the propensity to violate copyright law by sharing commercial software or copyright protected material. The sharing of copyright protected software and material is NOT allowed and is in direct violation of federal law and this AUP. Violation of the Peer to Peer policy shall trigger the Methods of Resolution under this AUP as set forth below in Table C.

Bit Torrent and Point-to-Point Software

Webnet allows the use of Bit Torrent and Point-to-Point ("P2P") software protocols on the public network. Webnet highly recommends strict oversight and management of Bit Torrent and P2P software environments due to the propensity to violate copyright law by sharing commercial software or copyright protected material. The sharing of copyright protected software and material is NOT allowed and is in direct violation of federal law and this AUP. Violation of the Bit Torrent and/or P2P policy shall trigger the Methods of Resolution under this AUP as set forth below in Table C.

The following list represents per se direct violations of this AUP and will be subject to immediate redress under one or more of the Methods of Resolution as described in this AUP and as set forth below in Table C. Note: Webnet is not required to follow the Methods of Resolution for Hourly Services, and reserves the right to immediately terminate Hourly Services based on violations of this AUP.

1. Copyright and Trademark Infringement: Direct copyright infringement (as defined and noted under Title 17, Section 512 of the United States Code) and trademark infringement are direct violations of Webnet's AUP. Please refer to DMCA copyright infringement requirements at http://www.Webnet.com/legal for filing complaints or counter notifications related to copyright claims.

Webnet International Company
Plot 110 Bukoto Street, Kamwokya
P.O.Box 34112, Kampala Uganda

Phone Numbers: +256772975207,
+256- 312105068, +256-414595955

Emails:sales@webnet.co.ug
Url:http://www.webnet.co.ug

2. Unsolicited Email: The sending or receiving of mass unsolicited email (SPAM) is a direct violation of Webnet's AUP. This includes the direct sending and receiving of such messages, support of such messages via web page, splash page or other related sites, or the advertisement of such services.

3. Email Bombing: The sending, return, bouncing or forwarding of email to specified user(s) in an attempt to interfere with or over flow email services is a direct violation of Webnet's AUP.

4. Proxy Email (SPAM): The use of dedicated services to proxy email unsolicited users is a direct violation of Webnet's AUP. Proxy email is defined as the use of dedicated services to act in concert with other services located inside and outside the network to achieve mass unsolicited email (SPAM) to unrelated third parties.

5. UseNet SPAM: The use of dedicated services to send, receive, forward, or post UseNet unsolicited email or posts is a direct violation of Webnet's AUP. This includes UseNet services located within the Webnet network or unrelated third party networks.

6. Illegal Use: Any use of dedicated services in a manner which is defined or deemed to be statutorily illegal is a direct violation of Webnet's AUP. This includes, but is not limited to: death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, "ponzi schemes", invasion of privacy, credit card fraud, racketeering, and other common illegal activities.

7. Child Pornography: Webnet has a zero-tolerance policy on child pornography and related sites. The hosting of child pornography or related sites or contact information is in direct violation of federal law and Webnet's AUP.

8. Threats & Harassment: The Webnet network can be utilized for any type of individual, organizational or business use. This does not include threats to or harassment of individuals, organizations or businesses, unless it falls within the bounds of protected free speech under the First Amendment of the United States Constitution. Webnet seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.

9. Fraudulent Activities: Webnet prohibits utilizing dedicated services or network services for fraudulent activities. Participation in fraudulent activities is in direct violation of state and federal law and Webnet's AUP.

10. Denial of Service: Webnet absolutely prohibits the use of dedicated services or network services for the origination or control of denial of service attacks or distributed denial of service attacks. Any relation to DOS or DDOS type activity is a direct violation of Webnet's AUP.

11. Terrorist Websites: Webnet prohibits the use of dedicated services for the hosting of terrorist-related web sites. This includes sites advocating human violence and hate crimes based upon religion, ethnicity, or country of origin.

12. Distribution of Malware: Webnet prohibits the storage, distribution, fabrication, or use of malware, including without limitation, virus software, root kits, password crackers, adware, key stroke capture programs and other programs normally used in malicious activity. Programs used in the normal ordinary course of business are deemed acceptable. Example: Security Company hosting at Webnet analyzes the latest root kit for new security analysis/software.

13. Phishing: Webnet strictly prohibits any activity associated with Phishing or systems designed to collect personal information (name, account numbers, usernames, passwords, etc.) under false pretense. Splash pages, phishing forms, email distribution, proxy email or any relation to phishing activities will result in immediate removal.

14. HYIP or Ponzi Schemes: High Yield Investment Plans or Ponzi schemes with the intent to defraud end users are illegal and not allowed on the network. This includes hosting, linking and or advertising via email websites or schemes designed to defraud.

15. Webnet will comply with and respond to jurisdictionally valid (as Webnet determines in its sole discretion) subpoenas, warrants, and/or court orders. If allowed, Webnet will forward such subpoenas, warrants, and/or orders to Customer and Customer may respond; however, Webnet reserves the right to respond as long as it is the named party in such subpoena, warrant, and/or order.

Webnet International Company
Plot 110 Bukoto Street, Kamwokya
P.O.Box 34112, Kampala Uganda

Phone Numbers: +256772975207,
+256- 312105068, +256-414595955

Emails:sales@webnet.co.ug
Url:http://www.webnet.co.ug

Reporting Violation of the Acceptable Use Policy

Webnet accepts reports of alleged violations of this AUP via email sent to abuse@Webnet.com. Reports of alleged violations must be verified and must include the name and contact information of the complaining party, and the IP address or website allegedly in violation, and description of the violation. Unless otherwise required by law, such as the DMCA, Webnet owes no duty to third parties reporting alleged violations due to lack of privity in contract law. Webnet will review all verified third party reports and will take appropriate actions as described within Methods of Resolution as set forth in Table C below or within its sole discretion.

Webnet understands the challenges of hosting companies, resellers, businesses, organizations and other customers who may have third party violations occur due to the nature of their business. The goal of our Methods of Resolution is to mitigate service interruptions while resolving potential violations under this AUP. Our sales, support and abuse staffs are dedicated to working with the Customer in resolving potential violations, and are available via phone, ticket, or email. The Methods of Resolution below form the framework for resolving all potential violations. Timing for resolution differs according to the degree of the violation, the nature of the violation, involvement of law enforcement, involvement of third party litigation, or other related factors. Overall, Webnet is dedicated to working with the Customer in resolving all potential violations prior to any service interruptions.

Step 1: First alleged violation of AUP: a ticket will be generated under Webnet to provide the Customer's master user with information regarding the potential violation of Webnet's AUP. This is often a fact-finding email requiring further information or notifying Customer of the potential violation and the required actions to resolve the issue.

Step 2: Acknowledgement of violation of AUP: a ticket is generated under the Customer's master user account with information specific to the violation. This ticket will also include any additional facts about the situation and will notify Customer of the action required to resolve the violation.

Step 3: Violation of AUP disregarded, not properly addressed, or continuing violation if a ticket has been disregarded, not properly addressed, or resolved by the Customer for a specified period of time: Webnet engineers will turn the public network port to the specified dedicated services off. Access to the dedicated services may then be achieved through the secure private service network for Customer resolution. As soon as the violation is addressed, the public access shall be restored and service will continue as normal.

Step 4: Failure to address violation and resolve violation: if Customer fails to address the violation AND fails to resolve the violation, a suspension of services shall occur. This is a last resort for Webnet and only results when the Customer completely fails to participate in Webnet's resolution process. A permanent suspension of services includes reclamation of all dedicated services and the destruction of Customer's data.