



info@joytel.net

ACCEPTABLE USE POLICY (AUP)

General Statement: JOYTEL 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) is the internet's single most valuable feature. JOYTEL is dedicated to protecting the source and distribution of information and protecting the rights and privileges of those utilizing it. JOYTEL 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. Notwithstanding anything found herein, JOYTEL 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 many customers, this AUP is intended to act as a guideline to service and not to be all encompassing.

Public Network: 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 the section below titled "Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy".

Private Network: The primary purpose of the JOYTEL Private Network is to allow secure private network connectivity to the private backend network directly connecting Customer servers and JOYTEL 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 JOYTEL 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 the section below titled "Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy".

Security Services: The primary purpose of the JOYTEL standard security services is to assist the Customer in the protection, management, update, and overall stability of the outsourced IT environment. JOYTEL also monitors all aggregate network traffic via Arbor networks and router netflow statistics for traffic analysis.

DNS Services: JOYTEL 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 JOYTEL 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, JOYTEL 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 the section below titled "Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy".

IP Addresses: All Internet Protocol (IP) Addresses are owned and managed by JOYTEL. IP Addresses are non-transferable from JOYTEL, and Customer retains no ownership or transfer rights to IP Addresses. All IP Addresses are assigned by the JOYTEL 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. All IP Addresses are currently registered to JOYTEL via ARIN assignments. Private IP assignments are available to qualified Customers.

Initial _____



info@joytel.net

IRC: JOYTEL allows the use of private internet relay chat (IRC) servers for communication among private parties. JOYTEL 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 the section below titled "Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy".

Peer to Peer: JOYTEL allows the use of internet peer to peer software for file sharing purposes. JOYTEL 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 the section titled "Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy".

Bit Torrent and Point-to-Point Software: JOYTEL allows the use of bit torrent and point-to-point ("P2P") software protocols on the public network. JOYTEL 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 the section titled "Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy".

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.

Note: SLA credits for Hourly Services will be calculated and applied based on the same monthly calculation used for the month-to-month contracts.

- 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 JOYTEL's AUP.
- 2. Unsolicited Email:** The sending or receiving of mass unsolicited email (SPAM) is a direct violation of JOYTEL'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 JOYTEL's AUP.
- 4. Proxy Email (SPAM):** The use of dedicated services to proxy email unsolicited users is a direct violation of JOYTEL'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 JOYTEL's AUP. This includes UseNet services located within the JOYTEL 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 JOYTEL's AUP. This includes, but is not limited to: death threats, terroristic threats, and threats of harm to other individuals, multi-level marketing schemes, "ponzi schemes", invasion of privacy, credit card fraud, racketeering, and other common illegal activities.
- 7. Child Pornography:** JOYTEL 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 JOYTEL's AUP.
- 8. Threats & Harassment:** The JOYTEL 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. JOYTEL seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.
- 9. Fraudulent Activities:** JOYTEL prohibits utilizing dedicated services or network services for fraudulent activities. Participation in fraudulent activities is in direct violation of state and federal law and JOYTEL's AUP.

Initial _____



info@joytel.net

10. Denial of Service: JOYTEL 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 JOYTEL's AUP.

11. Terrorist Websites: JOYTEL 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: JOYTEL prohibits the storage, distribution, fabrication, or use of malware including 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 JOYTEL analyzes the latest root kit for new security analysis/software.

13. Phishing: JOYTEL 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.

Disclosure of Customer Information: Occasionally, JOYTEL is required by law to submit Customer information to others, including law enforcement officials, when presented with a valid subpoena or order from a court or governmental entity with proper jurisdiction and authority. Information requested is disclosed only as directed pursuant to the subpoena or order. JOYTEL utilizes great care in keeping Customer information safe and private and will only release information described in the subpoena or order. JOYTEL will notify Customer of the information request as, and if, allowed by the subpoena or order.

Reporting Violation of the Acceptable Use Policy: JOYTEL accepts reports of alleged violations of this AUP via email sent to support@joytel.net. 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. JOYTEL owes no duty to third parties reporting alleged violations due to lack of privity in contract law. JOYTEL will review all verified third party reports and will take appropriate actions as described within Methods of Resolution as set forth in Table D below or within its sole discretion.

Methods of Resolution for Violations of JOYTEL's Acceptable Use Policy: The ultimate goal of JOYTEL is to balance the rights and interest of our Customers in the highly evolving internet world. JOYTEL 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 staff is dedicated to working with the Customer in resolving potential violations, and are available via phone 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, JOYTEL 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 JOYTEL to provide the Customer's master user with information regarding the potential violation of JOYTEL'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.

Initial _____



info@joytel.net

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: JOYTEL engineers will turn the public network port or 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 resolve the violation, a suspension of services shall occur. This is a last resort for JOYTEL and only results when the Customer completely fails to participate in JOYTEL's resolution process. A permanent suspension of services includes reclamation of all dedicated services and the destruction of Customer's data.

Disclaimer: JOYTEL retains the right, at its sole discretion, to refuse new service to any individual, group, or business. JOYTEL also retains the right to discontinue service with notice for repeated violation of the acceptable use policy over time.

Customer Signature

Date

Authorized JOYTEL Representative

Date