

Acceptable Use Policy (AUP)

General Statement: DrupalValueHosting.com 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. DrupalValueHosting.com is dedicated to protecting the source and distribution of information and protecting the rights and privileges of those utilizing it. DrupalValueHosting.com 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, DrupalValueHosting.com 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 the acceptable use policy is to inform all Customers of anticipated customer use. Due to the myriad of possibilities in maintaining a network comprised of thousands of servers, this document is intended to act as a guideline to service and not to be all encompassing.

Public Network: The primary purpose of the DrupalValueHosting.com 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 you do 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 will result in a violation of the AUP and shall result in methods of resolution under the acceptable use policy.

Private Network: The primary purpose of the DrupalValueHosting.com private network is to allow secure private network connectivity to the private backend network directly connecting Customer servers and Company 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 Company 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 will result in a violation of the AUP and shall result in methods of resolution under the acceptable use policy.

Security Services: The primary purpose of the DrupalValueHosting.com standard security services is to assist the Customer in the protection, management, update, and overall stability of the outsourced IT environment. All DrupalValueHosting.com services include network intrusion detection systems and denial of service mitigation via technology from 3Com (Tipping Point). These services are free of charge and are intended to mitigate or remove security risks associated with their perspective technologies. DrupalValueHosting.com also monitors all aggregate network traffic via Arbor networks and router netflow statistics for traffic analysis. DrupalValueHosting.com also supplies Microsoft update servers and Redhat 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 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 hosting accounts 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 the acceptable use policy.

Server Content: DrupalValueHosting.com does not actively monitor server content for review. DrupalValueHosting.com believes in the free dissemination of information via our services. Server content will only be reviewed upon complaint by verified third parties. Content that does not violate local, state and federal law or the acceptable use policy is deemed in compliance and shall remain intact. Legal adult content is allowed on DrupalValueHosting.com's servers. Content deemed in violation will be addressed pursuant to the methods of resolution under the acceptable use policy.

DNS Services: DrupalValueHosting.com 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 DrupalValueHosting.com 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, DrupalValueHosting.com will notify Customer of potential violation of the acceptable use policy. Customers requiring such DNS services will be instructed to perform dedicated DNS services on customer managed equipment. Violation of DNS services will result in methods of resolution under the acceptable use policy.

IP Addresses: All Internet Protocol (IP) Addresses are owned and managed by DrupalValueHosting.com. IP Addresses are non-transferable from DrupalValueHosting.com and Customer retains no ownership or transfer rights to IP Addresses. All IP Addresses are assigned by the DrupalValueHosting.com 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 the acceptable use policy. Violation of the IP Address policy will result in methods of resolution under the acceptable use policy. All IP Addresses are currently registered to DrupalValueHosting.com Technologies Inc. via Arin.net assignments. Private IP assignments are available to qualified Customers.

Acceptable Use Policy (AUP)

The following list represents per se direct violations of Acceptable Use Policy and will be subject to immediate redress under the methods of resolution as described in the acceptable use policy.

1. Copyright Infringement: Direct copyright infringement as defined and noted under Title 17, Section 512 of the United States Code are a direct violation of the acceptable use policy. Please refer to DMCA copyright infringement requirement <http://www.drupalvaluehosting.com/legal.html>.
2. Unsolicited Email: The sending or receiving of mass unsolicited email (SPAM) is a direct violation of the acceptable use policy. 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 the acceptable use policy.
4. Proxy Email (SPAM): The use of dedicated services to proxy email unsolicited users is a direct violation of the acceptable use policy. 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 the acceptable use policy. This includes UseNet services located within the DrupalValueHosting.com network or unrelated third party networks.
6. Illegal Use: Any use of dedicated services in direct attempt of statutory illegal activities is a direct violation of the acceptable use policy. 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, defamation, slander, and other common illegal activities.
7. Child Pornography: DrupalValueHosting.com has a zero stance 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 the acceptable use policy.
8. Threats & Harassment: DrupalValueHosting.com network can be utilized for any type of individual, organizational or business use. This does not include threats or harassment to individuals, organizations or businesses unless it falls within the bounds of protected free speech under the first amendment. DrupalValueHosting.com seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.
9. Fraudulent Activities: DrupalValueHosting.com prohibits utilizing dedicated services or network services for fraudulent activities. Notification of fraudulent activities by verified third parties can result in violation of the acceptable use policy.
10. Denial of Service: DrupalValueHosting.com 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 the acceptable use policy.
11. Terrorist Websites: DrupalValueHosting.com prohibits the use of dedicated services for the hosting of terrorist related websites. This includes sites advocating human violence and hate crimes based upon religion, ethnicity, or country of origin.
12. Distribution of Malware: DrupalValueHosting.com 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 DrupalValueHosting.com analyzes the latest root kit for new security analysis\ software.
13. Phishing: DrupalValueHosting.com 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 to Law Enforcement: Occasionally, DrupalValueHosting.com is required by law to submit customer information to law enforcement officials when presented with a valid subpoena from a court with proper jurisdiction. Information requested is disclosed as directed pursuant to the subpoena. DrupalValueHosting.com utilizes great care in keeping customer information safe and private and will only release information described in the subpoena. DrupalValueHosting.com will notify customer of the information request as allowed by the subpoena.

Acceptable Use Policy (AUP)

Reporting Violation of the Acceptable Use Policy: DrupalValueHosting.com accepts reports of alleged violations of the acceptable use policy via email sent to abuse@drupalvaluehosting.com. Reports of alleged violations must be verified and include name, contact information, IP address, and description of the violation. DrupalValueHosting.com owes no duty to third parties reporting alleged violations due to lack of privity in contract law. DrupalValueHosting.com will review all verified third party reports and will take appropriate actions as described within the acceptable use policies.

Privacy Agreement

Methods of Resolution for Violations under the Acceptable Use Policy: The ultimate goal of DrupalValueHosting.com is to balance the rights and interest of our customers in the highly evolving internet world. DrupalValueHosting.com 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 to our methods of resolution is to mitigate any service interruptions while resolving any potential violations under the policy. Our sales, support and abuse staff are dedicated to working with you in resolving potential violations and are available via phone or email. The methods of resolution below form the framework for a 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, DrupalValueHosting.com 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 email will be generated under the master user account with information regarding the potential violation of the acceptable use policy. 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: Violation of AUP disregarded, not properly addressed, or continuing violation if an email has been disregarded, not properly addressed, or resolved by the customer for a specified period of time, DrupalValueHosting.com engineers will turn the public network port to the specific dedicated services off. Access to the dedicated services is achieved through the secure private service network for Customer resolution. As soon as the violation is addressed, the public access is restored and service continues as normal.

Step 3: Failure to address violation and remove violation: if customer fails to address the violation AND resolve the violation, a suspension of services will occur. This is a last resort for DrupalValueHosting.com and requires a complete failure in the resolution process on behalf of the Customer. A permanent suspension of services includes reclamation of all dedicated services and data destroyed at the end of the current billing cycle.

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