



## Acceptable Use Policy

**General Statement:** Peak Hosting's 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. Peak Hosting 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. As such, this AUP is intended to act as a guideline to service and not to be all encompassing.

**Public Network:** The primary purpose of the Peak Hosting 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 Resolution Process as set forth in Exhibit A.

**Security Services:** The primary purpose of the Peak Hosting standard security services is to assist the Customer in the protection, management, update, and overall stability of the outsourced IT environment. 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 Resolution Process as set forth in Exhibit A.

**Server Content:** Peak Hosting does not actively monitor dedicated server content for review. 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 Peak Hosting dedicated servers. Content deemed in violation will be addressed pursuant to the Resolution Process as set forth in Exhibit A.

**DNS Services:** Peak Hosting 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 Peak Hosting with Customer specific domain name management through the Customer Ticketing System. In rare instances, where extreme intensive loads (DNS lookups) utilize disproportionate resources of the redundant DNS systems, Peak Hosting 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 Resolution Process as set forth in Exhibit A.

**IP Addresses:** All Internet Protocol (IP) Addresses are owned and managed by Peak Hosting. IP Addresses are non-transferable from Peak Hosting, and Customer retains no ownership or transfer rights to IP Addresses. All IP Addresses are assigned by the Peak Hosting 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 Resolution Process as set forth in Exhibit A. All IP Addresses are currently registered to Peak Hosting via ARIN assignments. Private IP assignments are available to qualified Customers.

**IRC:** Peak Hosting allows the use of private Internet Relay Chat (IRC) servers for communication among private parties. Peak Hosting 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 Resolution Process as set forth in Exhibit A.

**Peer to Peer:** Peak Hosting does not allow the use of internet Peer-to-Peer software for file sharing purposes. 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 Resolution Process as set forth in Exhibit A.

**Bit Torrent and Point-to-Point Software:** Peak Hosting does not allow the use of Bit Torrent and Point-to-Point ("P2P") software protocols on the public network. 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 Resolution Process as set forth in Exhibit A.

The following list represents per se direct violations of this AUP and will be subject to immediate redress under the Resolution Process described in this AUP and as set forth below in Exhibit A.

**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 Peak Hosting's AUP.

**2. Unsolicited Email:** The sending or receiving of mass unsolicited email (SPAM) is a direct violation of Peak Hosting'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 Peak Hosting's AUP.

**4. Proxy Email (SPAM):** The use of dedicated services to proxy email unsolicited users is a direct violation of Peak Hosting'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 Peak Hosting's AUP. This includes UseNet services located within the Peak Hosting 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 Peak Hosting'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:** Peak Hosting 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 Peak Hosting's AUP.

**8. Threats & Harassment:** The Peak Hosting 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. Peak Hosting seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.

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

**10. Denial of Service:** Peak Hosting 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 Peak Hosting's AUP.

**11. Terrorist Websites:** Peak Hosting 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:** Peak Hosting 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 Peak Hosting analyzes the latest root kit for new security analysis/software.

**13. Phishing:** Peak Hosting 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.

**Reporting Violation of the Acceptable Use Policy:** Peak Hosting accepts reports of alleged violations of this AUP via email sent to [abuse@peakwebhosting.com](mailto:abuse@peakwebhosting.com). Reports of alleged violations must be verified and must include the name and contact information of the complaining party, the IP address or website allegedly in violation, and description of the violation. Unless otherwise required by law, such as the DMCA, Peak Hosting owes no duty to third parties reporting alleged violations due to lack of privity in contract law. Peak Hosting will review all verified third party reports and will take appropriate actions as described within the Resolution Process as set forth in Exhibit A below or within its sole discretion.



## Exhibit A

### Resolution Process for PH AUP Violations

Peak Hosting 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 Resolution Process is to mitigate service interruptions while resolving potential violations under this AUP. The Resolution Process below forms 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, Peak Hosting 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 Peak Hosting to provide the Customer's master user with information regarding the potential violation of Peak Hosting'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:** Peak Hosting 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 Peak Hosting and only results when the Customer completely fails to participate in Peak Hosting's resolution process. A permanent suspension of services includes reclamation of all dedicated services and the destruction of Customer's data.

**Disclaimer:** Peak Hosting retains the right, at its sole discretion, to refuse new service to any individual, group, or business. Peak Hosting also retains the right to discontinue service to Customers with excessive and/or multiple repeated violations.