

ACCEPTABLE USE POLICY (AUP):

This Acceptable Use Policy (AUP) is incorporated by reference in your Master Service Agreement with ServerIntelligent. Your services may be suspended or terminated for violation of this AUP in accordance with your service agreement.

1. **Overview:** Our goal is to deliver enterprise quality services to all of our Customers. ServerIntelligent is dedicated to protecting the source and distribution of information and protecting the rights and privileges of those utilizing the Internet including the storage, distribution, and exchange of information (content). ServerIntelligent has no intent on acting as the content police; our duty in the process of information dissemination is simply to act as conduit between interested parties. Notwithstanding anything found herein, ServerIntelligent 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 many possibilities in maintaining a network comprised of thousands of servers, this AUP is intended to act as a guideline to service and not all encompassing.
2. **Mail Requirements:** Customers must comply with the CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial email. These policies apply to messages sent using your ServerIntelligent' services, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site or an email address hosted via your ServerIntelligent service. In addition, you may not use a third party email service that does not practice similar procedures for all its customers. These requirements apply to distribution lists prepared by third parties to the same extent as if the list were created by you. In addition, your bulk and commercial email must meet the following requirements:
 - a. Your intended recipients have given their consent to receive email from you via some affirmative means, such as an opt-in procedure.
 - b. Your procedures for seeking consent include reasonable means to ensure that the person giving consent is the owner of the email address for which consent is given.
 - c. You retain evidence of each recipient's consent in a form that can be promptly produced on request.
 - d. You have procedures in place that allow a recipient to revoke their consent - such as a link in the body of the email, or instructions to reply with the word "Remove" in the subject line; you honor revocations of consent within 48 hours, and you notify recipients that the revocation of their consent will be implemented in 48 hours.
 - e. You must post an email address for complaints (such as abuse@yourdomain.com) in a conspicuous place on any website associated with the email, you must register that address at abuse.net, and you must promptly respond to messages sent to that address.
 - f. You may not obscure the source of your email in any manner, such as omitting, forging, or misrepresenting message headers or return addresses. Your email must include the recipient's email address in the body of the message or in the "TO" line of the email. The subject line of the email must clearly describe the subject matter contained in the email, and the message must include valid contact information.
 - g. ServerIntelligent will handle all complaint resolution with upstream bandwidth providers and anti-spam organizations related to Customer's use of ServerIntelligent' IP's and Bandwidth. ServerIntelligent shall provide Customer with an email notification of any complaints received, and Customer shall a) provide ServerIntelligent, Inc. with all opt-in information related to such complaint within twenty-four (24) hours; and b) permanently remove any associated end-user email addresses from all of Customer's opt-in email lists. Customer shall not add a Removed Address back onto its Lists or attempt to deliver any email to a Removed Address even if Customer receives a future opt-in request from such Removed Address. ServerIntelligent will not under any circumstances provide Customer's information to any upstream bandwidth providers, anti-spam organizations, or to ARIN for SWIP purposes unless specifically requested by Customer.
 - h. If a Spamhaus (<http://spamhaus.org/sbl>) SBL or UCE Protect Network Level 2 or 3 (<http://www.uceprotect.net>) listing occurs and removal of Customer from IP space is required immediately, or Upstream Provider null routes IP space due to complaints, there will be no refunds for services and Customer is responsible for paying entire Contract in full. In the case of a null route or SBL / UCE-Protect listing or any other client-activity-based cause resulting in the loss of the IP space, Customer agrees to forfeit the current month's service payment due to customer violation of the Acceptable Use Policy. Customer may, at ServerIntelligent's sole discretion, procure new IP space and service(s) under a new Service Order FORM.

3. **Direct AUP Violations:** The following list represents direct violations of this AUP:
 - a. **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.
 - b. **Illegal Use:** Any use of services in a manner which is defined or deemed to be statutorily illegal. 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.
 - c. **Child Pornography:** ServerIntelligent 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.
 - d. **Threats & Harassment:** The ServerIntelligent 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. ServerIntelligent seeks to serve only as the medium of exchange for information and refrains from decisions on freedom of speech.
 - e. **Fraudulent Activities:** ServerIntelligent prohibits utilizing services for fraudulent activities.
 - f. **Denial of Service:** ServerIntelligent prohibits the use of services for the origination or control of denial of service attacks or distributed denial of service attacks.
 - g. **Terrorist Websites:** ServerIntelligent prohibits the use of 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.
 - h. **Distribution of Malware:** ServerIntelligent 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.
 - i. **Phishing:** ServerIntelligent 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.
 - j. **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.
4. **Public Network:** The primary purpose of the ServerIntelligent Public Network is to transmit information 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.
5. **Private Network:** The primary purpose of the ServerIntelligent Private Network is to allow secure private network connectivity to the private backend network directly connecting Customer servers and ServerIntelligent 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 ServerIntelligent 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 nonpayment, 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 a restricted basis, and is a privilege not a right based on ServerIntelligent sole determination. 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.
6. **Security Services:** The primary purpose of the ServerIntelligent security services is to assist the Customer in the protection, management, update, and overall stability of their environment. ServerIntelligent monitors network and router statistics for traffic analysis. ServerIntelligent also supplies various patches and updates to switches and ServerIntelligent managed equipment. Many security services offered for a fee and are covered via the terms of the individual services. These services include, but are not limited to: firewalls, host intrusion detection services, 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 shall be considered a violation of the AUP.

7. **Server Content:** ServerIntelligent does not actively monitor dedicated server content for review. ServerIntelligent 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 ServerIntelligent dedicated servers. Content deemed in violation shall be considered a violation of the AUP.
8. **DNS Services:** ServerIntelligent supplies name services for most Customers purchasing dedicated services. These name services usually include the use of authoritative name servers for public resolution of domain names and private domain name resolvers located on our network. The DNS services are fully managed and maintained by ServerIntelligent 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, ServerIntelligent 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 be considered a violation of the AUP.
9. **IP Addresses:** All Internet Protocol (IP) Addresses are owned or leased and managed by ServerIntelligent. IP Addresses are non-transferable from ServerIntelligent, and Customer retains no ownership or transfer rights to IP Addresses. Attempted use of IP addresses not originally allocated for use or IP addresses used on non-assigned VLANs or servers is a violation of this AUP.
10. **IRC:** ServerIntelligent allows the use of private internet relay chat (IRC) servers for communication among private parties. ServerIntelligent 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.
11. **Peer to Peer:** ServerIntelligent allows the use of internet peer to peer software for file sharing purposes. ServerIntelligent highly recommends strict oversight 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.
12. **Bit Torrent:** ServerIntelligent allows the use of bit torrent protocols on the public network. ServerIntelligent highly recommends strict oversight and management of bit torrent 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.
13. **Unauthorized Access:** Use of the ServerIntelligent' services to access, or to attempt to access the accounts of others, or to penetrate, or attempt to penetrate security measures of ServerIntelligent or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data, is expressly prohibited and the offending account is subject to immediate termination. The outstanding balance of any contracts / account will immediately become due.
14. **Reporting Violation of the Acceptable Use Policy:** ServerIntelligent accepts reports of alleged violations of this AUP via email sent to abuse@serverintelligent.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. ServerIntelligent owes no duty to third parties reporting alleged violations due to lack of privacy in contract law. ServerIntelligent will review all verified third party reports and will take appropriate actions.