Last modified: 2/1/2016

MacStadium, Inc.

Acceptable Use Policy

To protect the interests of all clients and ensure optimal service levels, MacStadium, Inc. ("MacStadium") has developed the following Acceptable Use Policy ("AUP"), which applies to all clients and customers (and their respective users) (collectively, "Clients") of MacStadium. Use of any service offered by MacStadium by any Client will constitute acknowledgment of, and agreement to, the terms outlined in this AUP. This AUP may be revised in part or in full at any time by MacStadium. Continued use of MacStadium's services after such changes have been made to the AUP will constitute acceptance of any revisions to the AUP.

Clients may only use our servers for lawful purposes, in compliance with all applicable federal, state and local laws or regulations and in compliance with this AUP.

Specific activities that are prohibited include, but are not limited to:

- Hosting, storage or transmittal of any material in violation of any applicable law or regulation, including without limitation, libel, defamation of character, invasion of privacy and tortious interference.
- Hosting, storage or transmittal of any material protected by copyright, trademark, trade secret or any other intellectual property right without proper authorization.
- Hosting, storage or transmittal of any material legally judged to be threatening or obscene, pornography or sexually explicit material that is in violation of any applicable federal, state or local law or regulation, such as material that involves the depiction or use of underage persons.
- Transmitting adult content to juvenile users of the Internet.
- Exporting technical or military data to prohibited countries.
- Violating United States export control laws or regulations for software or technical information or violating United States laws or regulations concerning the doing of business with certain designated persons or entities.
- Failing to provide complete, truthful and accurate information regarding the Client's identity as requested on all of MacStadium's application forms.
- Misrepresenting or fraudulently representing products/services.
- Threatening harm to persons or property or otherwise harassing behavior.
- Abusing or harassing MacStadium employees, staff or agents, including without limitation, verbal harassment, yelling, swearing, rudeness, threats or any intentionally disruptive behavior.
- Hosting, storage or transmittal of any material that sponsors, assists in or encourages the unlawful use or threatened use of force or violence against persons or property to intimidate or coerce a government, any civilian population or any segment thereof, in furtherance of political or social objectives.
- Managing a proxy server on MacStadium's network.
- Being subject to economic sanctions, prohibitions or restrictions on trade or export imposed by any governmental authority having jurisdiction over Client or MacStadium, or in any jurisdiction where MacStadium or any of its affiliates are located ,and whether or not the services provided to Clients by MacStadium or such affiliate would violate such economic sanctions, prohibitions or restrictions.

- Interfering with the legitimate use by Clients or other third parties of resources on the MacStadium network or any of MacStadium's services.
- Facilitating, aiding or encouraging any of the above prohibited activities, whether using MacStadium's network or any other network.

SPAM AND UNSOLICITED COMMERCIAL EMAIL

The Client must comply with the CAN-SPAM Act of 2003 and all relevant regulations and legislation on bulk and commercial email. MacStadium takes a zero tolerance approach to the sending of mass Unsolicited Commercial Email ("UCE") or spam over our network. UCE is any email message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service, which is sent to a recipient who has not requested it or opted out of such communication.

This means that Clients of MacStadium may not use or permit others to use our network to transact in UCE. In order to prevent unnecessary blacklisting due to spam, we reserve the right to occasionally sample bulk email being sent from servers.

To reiterate the strength of our zero tolerance approach to the sending of UCE or spam over our network, the following activities are strictly prohibited:

- **General Prohibitions.** Using the MacStadium network to send or receive replies from UCE; hosting sites or information that is advertised by UCE from other networks; transmitting bulk email through remote SOCKS, HTTP or other similar proxies who in turn make a SMTP connection to the destination mail servers; forging email headers (i.e., "spoofing"); spamming using third-party proxy, aggregation of proxy lists, or proxy mailing software installation; or hosting any web pages or providing any services that support spam.
- **Landing Sites.** The hosting of any web site or other content in any form intended to be intentionally or unintentionally retrieved or viewed by any recipient of any unsolicited email sent in violation of the spirit or letter of the terms defined in this document, whether sent from our network or any other network.
- **Newsgroup Spamming.** The posting of commercial messages to any newsgroup or discussion forum not chartered or organized for that specific purpose.

SYSTEM AND NETWORK SECURITY

The Client is required to protect the security of its Internet accounts (ftp, email, etc.) and usage to ensure the security of the MacStadium network and every MacStadium network object, including without limitation, routers, switches and workstations. Further, the Client is responsible for validating the integrity of the information and data it receives or transmits over the Internet and reporting any weaknesses in the MacStadium network and any incidents of possible misuse or violation of this AUP.

To ensure the integrity of our network, the following activities are strictly prohibited:

- **General Prohibitions.** Using or distributing tools designed to compromise security; unauthorized monitoring of data or traffic on the MacStadium network or any other network without express authorization, deliberate attempts to overload the MacStadium network and broadcast attacks; forging of any TCP-IP packet header or any part of the header information in an email or intentionally or negligently transmitting files containing a computer virus or corrupted data.
- **Denial of Service Attacks.** The launching or facilitating the launch of a denial of service ("DoS") attack on any host or computer on the MacStadium network for any reason whatsoever, or the use of any

MacStadium network resource to interfere with the legitimate use by Clients or other authorized users of resources of the MacStadium network or any other network. This includes the hosting of a Camfrog server or other server application that is a frequent target of DoS attacks or other types of attacks.

- **Port Scanning.** The scanning of the service ports of any host or computer on the MacStadium network or any other network, or the sniffing of packet traffic on the MacStadium network. The placing of any network interface into promiscuous mode is similarly prohibited.
- **Unauthorized Access.** Any unauthorized access to or unauthorized alteration of the files or operating system or other content of any host or network, any unauthorized attempt to obtain login credentials, such as username and/or password, of any host on the MacStadium network or any other network or any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures.
- **IRC Networks.** The hosting of an IRC server that is part of or connected to another IRC network or server. Servers found to be connecting to or part of these networks will be immediately removed from our network without notice. The server will not be reconnected to the network until such time that Client agrees to completely remove any and all traces of the IRC server and agree to let us have access to Client's server to confirm that the content has been completely removed.

RESOURCE USAGE

Client agrees that bandwidth usage shall not exceed the number of gigabytes per month for the services ordered by Client. MacStadium will monitor Client's bandwidth usage and will provide real time graphs of bandwidth usage for Client to review in the MacStadium client portal. MacStadium shall have the right to take corrective action if Client's bandwidth usage exceeds the amount allocated by Client's service plan ("Allocation"). Bandwidth usage is measured on a monthly basis coinciding with Client's billing cycle. Both incoming and outgoing traffic are counted towards the total number of gigabytes per month for the services ordered by Client. Unused bandwidth allocations cannot be carried over to future months, or applied to other servers or accounts.

Should a Client's bandwidth usage exceed the Client's Allocation, the following corrective actions may be taken and additional charges may be assessed:

- Corrective action may include the assessment of additional charges, disconnection or discontinuance of any and all services, or termination of this AUP and the Terms of Service, which may be taken in MacStadium's sole and absolute discretion. MacStadium believes in communicating with our Clients and will try to work with our Clients to resolve any overage issues before taking action which could cause a Client's service to become unavailable.
- In the event that a Client exceeds the included Allocation, MacStadium may, at its sole discretion, collect a deposit in the amount of $0.10 per GB for the projected overage for the month, immediately against Client's credit card on file with MacStadium.
- Client agrees to pay MacStadium any additional fees for bandwidth overages within thirty (30) days of the invoicing period at a rate of $0.10 per GB of bandwidth used over the Allocation. Any bandwidth overage bill not paid within thirty (30) days of invoicing will subject the server and services to suspension.

IP Allocations

All IP addresses which are assigned to Client must be justified per ARIN Guidelines at http://www.arin.net/policy/nrpm.html. If it is determined that IP addresses which have been assigned to Client are not being used in accordance with these guidelines, they may be revoked.

IMMEDIATE THREATS

If, in the reasonable determination of MacStadium, the equipment, software or hosted applications used by the Client or the activities of the Client poses an immediate threat to the physical integrity of MacStadium premises or the physical integrity or performance of the equipment or network of MacStadium or any other user of the premises, or poses an immediate threat to the safety of any person, then MacStadium may perform such work and take such other actions that it may consider necessary without prior notice to the Client and without liability for damage to the equipment or data for any interruption of the Client's (or its Clients') businesses. As soon as practical after performing such work, MacStadium will advise, by email, the Client of the work performed or the action taken.

MONITORING

To determine compliance with this AUP and our Terms of Service, MacStadium reserves the right to monitor Client usage of the MacStadium network, including without limitation, occasionally sampling bulk email and monitoring bandwidth usage. Client hereby consents to such monitoring and agrees that MacStadium is under no duty under this AUP, the Terms of Service, or otherwise, to monitor Client use of MacStadium services.

CLIENT'S RESPONSIBILITY FOR ITS USERS

Any act or omission by a Client's customers or users will be a breach of this AUP if the act committed by the customer or user would be deemed a breach of this AUP if committed by Client.

VIOLATION

Violation of MacStadium's AUP will result in severe penalties. MacStadium may initiate an immediate investigation to substantiate the alleged violation. During the investigation, MacStadium may restrict Client access to the network to prevent further violations. The designation of any materials and actions as prohibited as described in this AUP is left entirely to the discretion of MacStadium management.

If a Client is found to be in violation of our AUP, MacStadium may, at its sole discretion, restrict, suspend or terminate such Client's account. MacStadium has no obligation to provide warnings under any circumstances and can terminate the Client's account without prior notification upon a finding that the Client has violated this AUP. Further, MacStadium reserves the right to pursue civil remedies for any costs associated with the investigation of a substantiated policy violation. MacStadium will notify law enforcement officials if the violation is believed to be a criminal offense and will cooperate fully with law enforcement authorities in investigating the alleged criminal offense.

First violations of this policy will result in an "administrative fee" of $250 and the Client's account will be reviewed for possible immediate termination. A second violation will result in an administrative fee of $500 and immediate termination of the Client's account. Clients who violate this policy shall also be responsible for "research fees" in an amount of $175 per hour for all time that MacStadium personnel must spend to investigate the matter.