

**Exhibit B****ACCEPTABLE USE POLICY**

This Exhibit B – AUP is attached to and made a part of the Agreement made by and between Customer and MacStadium. Capitalized terms used but not defined in this AUP will have the meaning assigned to them in the Agreement.

To protect the interests of all Customers and ensure optimal Service Levels, MacStadium has developed this AUP, which applies to you, your Users, and all other Customers (and their respective Users) use of the Services offered by MacStadium. Use of any Services offered by MacStadium 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. Your continued use of MacStadium’s Services after such changes have been made to the AUP will constitute acceptance of any revisions to the AUP.

**1. PROHIBITED ACTIONS**

Customers 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. In addition to the restrictions concerning use of the Services pursuant to 2.4 of the Agreement, specific activities that are also 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 Customer’s identity as requested on all of MacStadium’s application forms.
- Misrepresenting or fraudulently representing any products or 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 Customer or MacStadium, or in any jurisdiction where MacStadium or any of its affiliates are located, and whether or not the Services provided to Customers by MacStadium or such affiliate would violate such economic sanctions, prohibitions or restrictions.
- Interfering with the legitimate use by Customers or other third parties of resources on the MacStadium network or any of MacStadium's Services.
- Storage, transmittal or use of any malicious code, such as viruses, worms, time bombs, Trojan horses and other harmful or malicious files, scripts, agents or programs
- Imitating or impersonating MacStadium or any of its employees, any other person or his or her email address or creating false accounts for the purpose of sending spam or phishing or any other violation pursuant to the CAN-SPAM Act.
- Sell, distribute or export illegal or prescription drugs or other controlled substances or paraphernalia.
- Intentional storage, transmittal or use of any materials that violates, encourages or furthers conduct that would violate any applicable laws, including any criminal laws, or any third-party rights, including publicity or privacy rights.
- Mine bitcoins and other cryptocurrencies.
- Use the Services in any manner that would disparage MacStadium in any way.
- Facilitating, aiding or encouraging any of the above prohibited activities, whether using MacStadium's network or any other network.

## 2. SPAM AND UNSOLICITED COMMERCIAL EMAIL

The Customer must comply with the CAN-SPAM Act of 2003 and all relevant regulations and legislation on bulk and commercial. MacStadium takes a zero-tolerance approach to the sending of mass Unsolicited Commercial Email ("**UCE**") or spam over our network. UCE is any message where the primary purpose is 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 Customers 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 regarding the sending of UCE or spam over our network, the following activities are strictly prohibited:

- General Prohibitions. a) Using the MacStadium network to send or receive replies from UCE, hosting sites or information that is advertised by UCE from other networks, b) transmitting bulk email through remote SOCKS, HTTP or other similar proxies who in turn make a SMTP connection to the destination mail servers, c) forging email headers (i.e., 'spoofing'), d) spamming using third-

party proxy, aggregation of proxy lists, or proxy mailing software installation, and e) 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 terms defined in this AUP, 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.

### 3. U.S. DIGITAL MILLENNIUM COPYRIGHT ACT OR SIMILAR STATUTORY OBLIGATIONS

To the extent a Customer uses the Services for hosting, advertising, sending electronic messages or for the creation and hosting of, or for posting material on, websites, each Customer must a) comply with any notices received under Title II of the Digital Millennium Copyright Act of 1998 (Section 512 of the U.S. Copyright Act) or similar statute in other countries (the "DMCA"), b) set up a process to expeditiously respond to notices of alleged infringement that comply with the DMCA and to implement a DMCA-compliant repeat infringers policy, and c) comply with such processes and policy(ies).

In appropriate circumstances, MacStadium will terminate the accounts of Customers who MacStadium suspects to be repeatedly or blatantly infringing copyrights. If MacStadium receives a notice alleging that Customer or Customer's Users are infringing another party's intellectual property, MacStadium may disable that Customer's access to the Service or remove the alleged infringing material. If MacStadium receives more than one such notice for the same customer, MacStadium reserves the right to immediately terminate such Customer's Subscriptions to the Services as deemed necessary by MacStadium to ensure continued protection under the safe harbor provisions under the DMCA or to prevent violations of other applicable laws or third parties' rights.

### 4. SYSTEM AND NETWORK SECURITY

The Customer is required to protect the security of its internet accounts (e.g. 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 Customer 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. a) Using or distributing tools designed to compromise security, b) 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, and c) 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 Customers 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 Customer agrees to completely remove any and all traces of the IRC server and agree to let us have access to Customer's server to confirm that the content has been completely removed.

## **5. IP ALLOCATIONS**

All IP addresses which are assigned to Customer 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 Customer are not being used in accordance with these guidelines, they may be revoked.

## **6. IMMEDIATE THREATS**

If, in the reasonable determination of MacStadium, the equipment, software or hosted applications used by the Customer or the activities of the Customer 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 deemed necessary without prior notice to the Customer and without liability for damage to the equipment or data for any interruption of the Customer's (or its Customers') businesses. As soon as practical after performing such work, MacStadium will advise, by email, the Customer of the work performed or the action taken.

## **7. MONITORING**

To determine compliance with this AUP and our Agreement, MacStadium reserves the right to monitor Customer usage of the MacStadium network. Customer hereby consents to such monitoring and agrees that MacStadium is under no duty under this AUP, the Agreement, or otherwise, to monitor Customer use of MacStadium Services.

## **8. CUSTOMER'S RESPONSIBILITY FOR ITS USERS**

Any act or omission by a Customer's customer or User will be a breach of this AUP if the act or omission committed by the customer or User would be a breach of this AUP if committed by Customer.

## **9. VIOLATION**

MacStadium may initiate an immediate investigation to substantiate the alleged violation. During the investigation, MacStadium may restrict Customer 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 reasonable discretion of MacStadium management.

If a Customer is found to be in violation of this AUP, MacStadium may, at its sole and reasonable discretion, restrict, suspend or terminate such Customer's account. MacStadium has no obligation to

provide warnings under any circumstances and can terminate the Customer's account without prior notification upon a finding that the Customer has violated this AUP. Further, MacStadium may 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 Customer'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 Customer's account. Customers who violate this policy shall also be responsible for 'research fees' in an amount of \$175 per hour for any time that MacStadium personnel must reasonably spend to investigate the matter.