# Acceptable Use Policy

This is a sub-agreement as part of a Master Service Agreement (MSA) that establishes and regulates the relationship between RACKEND and its customers. All customers ordering and/ or using RACKEND services must agree to be bound by the MSA. The MSA can be found at:

http://www.rackend.com/pdfs/RE_MSA.pdf

This Acceptable Use Policy is designed to protect the integrity, security, reliability, and privacy of the RACKEND networks and the products and services RACKEND offers to its customers. This policy applies to all customers (persons and entities) using the products and services of RACKEND. The use of RACKEND's products and services constitutes your acceptance of the Acceptable Use Policy in effect at the time of your use. All RACKEND customers agree not to engage in any unacceptable use of the service provided and assume all responsible for any and all acts and omissions that occur during or relating to their use of the service. RACKEND reserves the right to modify "The Acceptable Use Policy" at any time, effective immediately upon posting of the modification.

Forms of unacceptable may include, but are not limited to, the following:

1. Transmission, re-transmission, posting, and/or storing material on or through any of RACKEND products or services, if in the proprietary judgment of RACKEND, such transmission, retransmission, posting, or storage is: (a) in violation of any law/regulation of the Republic of Panama, and/or Switzerland (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations); (b) threatening and/or abusive; (c) indecent; (d) defamatory; or (e) obscene. Each RACKEND customer is and will remain responsible for determining what laws or regulations are applicable to his or her use of the services and products.

2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use

3. False or Misleading Representations and Deceptive Marketing Practices.

4. Any actions that can restrict or inhibit anyone - whether or not the customer is affiliated with RACKEND or otherwise - in his or her experience or use of RACKEND services and products, or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or standard business use of Internet services.

5. Any attempt to circumvent (bypass) user authentication or security of any host, network, or account. This includes, but is not limited to, probing the security of other networks, logging into a server or account the Customer is not expressly authorized to access or accessing data not intended for the customer.

6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the customer is not an intended recipient or logging into a server or account that the customer is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, and forged routing information for malicious purposes.

7. Port scanning or security scanning is expressly prohibited

8. Implementing any form of network monitoring that will intercept data not intended for the customer.

9. Introduction of malicious programs into the RACKEND network or servers or other products and services of RACKEND (e.g, viruses,worms, trojan horses, email bombs, etc.).

10. Hindering or denying service to any user other than the customer's host (for example, denial of service attack).

11. Supplying false or incorrect data on the required order form contract (electronic or paper) attempting to circumvent or change the processes or procedures to measure time including fraudulent use of credit card numbers or, bandwidth utilization or other actions to document "use" of RACKEND’s products or services.

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

13. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

14. The sending of unsolicited mail messages, including, but not limited to, any sending of "junk mail" or other advertising material to individuals who did not specifically request such material, and who were not previous customers of the customer or with whom the customer does not have an existing or corresponding business relationship (e.g., E-mail "spam"). Distributing, advertising, or promoting services or software that have the main objective of encouraging or even facilitating unsolicited commercial E-mail or “spam”.

15. Any possible form of forging of email header information or any unauthorized use of said information.

16. Any and all solicitations of any email address or mail, other than that of the poster's authorized account or expected service, with the general intent to collect replies or harass.

17. The forwarding or creating of "chain letters”, “pyramid”, or “Ponzi” schemes of any type.

18. Use of unsolicited E-mail originating from within RACKEND’s network of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by RACKEND or connected via the RACKEND network.

19. Any failure or delay in exercising or enforcing this policy does not in any way constitute a waiver of the policy or of any other right. Should any provision of this policy be deemed unenforceable due to law or change in law, that provision shall be disregarded at that time and the balance of the policy shall remain in effect in accordance with the law.

Abusable Resources

Any and all abuse of an open resource that occurs after the customer has received notification shall be considered a violation of the policy and enforced as such. Also, upon notification of the abusable resources existence (e.g., open news server, unsecured mail relay, or smurf amplifier), the RACKEND customer shall promptly take any and all necessary steps to avoid further abuse of such open resource.

Enforcement

RACKEND reserves the right to promptly suspend and/or terminate the RACKEN customer's established service for abuse of any provision of this policy upon verbal and/or written notice. Notice may be provided by voicemail or Email when applicable to the customer.

Before the subsequent suspension or termination of a customer, RACKEND will work with the customer to rectify any and all violations of the aforementioned policy while ensuring that there will be no re-occurrence; however, RACKEND reserves the right to suspend or terminate based on a first offense in any cases deemed necessary.