Acceptable Use Policy

This agreement is part of a Master Service Agreement (MSA) that governs the relationship between Private Layer and its customers. All customers ordering and using Private Layer services must agree to be bound by the MSA. The MSA can be found at:

http://www.privatelayer.com/pdfs/PL_MSA.pdf

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

Unacceptable use includes, but is not limited to, any of the following:

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

2. Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by customer.

3. Deceptive marketing practices.

4. Actions that restrict or inhibit anyone - whether a customer of Private Layer or otherwise - in his or her use or enjoyment of Private Layer products and services, or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or business use of Internet services.

5. Introduction of malicious programs into the Private Layer network or servers or other productsand services of Private Layer (e.g., viruses,trojan horses and worms).

6. Causing or attempting to cause security breaches or disruptions of Internet communications.Examples of 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. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.

7. Executing any form of network monitoring that will intercept data not intended for the customer.

8. Circumventing user authentication or security of any host, network or account.

9. Interfering with or denying service to any user other than the customer's host (e.g., denial of service attack).

10. Using any program/script/command, or sending messages of any kind, designed to interfere with, or to disable a user's terminal session.

11. Furnishing false or incorrect data on the order form contract (electronic or paper) including fraudulent use of credit card numbers or attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization or other methods to document "use" of Private Layer's products or services.

12. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers of the customer or with whom the customer does not have an existing business relationship (e.g., E-mail "spam"); or distributing, advertising or promoting software or services that have the primary purpose of encouraging or facilitating unsolicited commercial E-mail or spam.

13. Harassment, whether through language, frequency, or size of messages.

14. Unauthorized use or forging of mail header information.

15. Solicitations of mail or any other E-mail address other than that of the poster's account or service, with the intent to harass or collect replies.

16. Creating or forwarding "chain letters" or other "pyramid schemes" of any type.

17. Use of unsolicited E-mail originating from within the Private Layer network or networks of other Internet Service Providers on behalf of or to advertise any service hosted by Private Layer or connected via the Private Layer network.

18. No failure or delay in exercising or enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in law, such a provision shall be disregarded and the balance of the policy shall remain in effect.

Abusable Resources

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

Enforcement

Private Layer may immediately suspend and/or terminate the customer's service for violation of any provision of this policy upon verbal or written notice, which notice may be provided by voicemail or Email.

Prior to suspension or termination, Private Layer attempts to work with our customers to cure violations of this policy and ensure that there is no re-occurrence; however, Private Layer reserves the right to suspend or terminate based on a first offense