Acceptable Use Policy

1. General

Radiant Communications ("Radiant") provides a variety of data communication, Internet, hosting, email and related services (the "Services") via Radiant's equipment, interconnections with other carriers, systems, and facilities (the "Network"). This Acceptable Use Policy ("AUP") sets forth the allowed and appropriate uses of the Services and the Network by our customers ("Customers"), their customers, and their employees, contractors, or end-users, and any other parties who may use or access the Services or the Network (the "End-Users"). All Customers and their End-Users must comply with this AUP.

By letting its End-Users use or access the Services or Network, Customer agrees to be bound by the terms of this AUP. Any indirect or attempted violation of this policy by a Customer or its End-Users shall be considered a violation of the AUP by the Customer and the Customer shall be held directly accountable therefore.

Radiant reserves the right to change this AUP from time to time and will notify Customers by posting a revised copy of the AUP at http://legal.radiant.net/. Customers are responsible for ensuring their End-Users are aware of and comply with any such changes.

2. Radiant's Rights and Remedies

Radiant has no responsibility for any material or information created, stored, maintained, transmitted or accessible on or through the Services or Network and is not obligated to monitor or exercise any editorial control over such material. In the event that Radiant becomes aware that any such material may violate this AUP and/or expose Radiant to civil or criminal liability, Radiant reserves the right to investigate such material, block access to such material, and suspend or terminate any Services without advance notice or liability. Customer shall be liable for any Early Termination fees that may be incurred if Services are terminated under the provisions of this AUP.

Radiant reserves the right to cooperate with legal authorities of proper jurisdiction and third parties in investigating any alleged violations of this AUP, including disclosing the identity of any Customer or End-User that Radiant believes is responsible for such violation. Radiant also reserves the right to implement technical mechanisms to prevent violations of this AUP.

Nothing in this AUP shall limit in any way Radiant' rights and remedies at law or in equity that may otherwise be available.

3. Acceptable Use

Customers and their End-Users shall not use the Services or the Network to transmit, distribute or store material or conduct activities: (a) of an illegal or unlawful nature under the laws of Canada, the provinces of British Columbia or Ontario, or any other applicable jurisdiction; (b) that violates the terms of this AUP or any other applicable agreement with Radiant; (c) that interferes with or adversely affects the Services, Network, Internet, or the use of the Services or Network by other Customers; (d) that is threatening or defamatory or otherwise injurious to the business or reputation of others; or (e) that may expose Radiant to criminal or civil liability. Customers shall cooperate with Radiant in investigating and correcting any apparent breach of this AUP. Customers shall be solely responsible for any material that their End-Users store, transmit, download, view, post, distribute or otherwise access or make available using the Services or Network.

In particular, but without limiting the more general prohibitions in this AUP, Customers and their End-Users shall not use the Services or Network, or assist anyone else to:

1. Conduct activities, or transmit, distribute or store data or materials that, as reasonably determined by Radiant:(a) are obscene, defamatory, threatening, abusive, advocating violence or which violate a law, regulation or public policy; (b) solicit or exploit minors for sexual or pornographic acts; (c) might be harmful

to or interfere with Radiant's Services, Network, the Internet, or any third party's networks, equipment, applications, services, or web sites (e.g., viruses, worms, Trojan horses, etc.); (d) would infringe, dilute, misappropriate, or otherwise violate any privacy, intellectual property, publicity or other personal rights including, without limitation, copyrights, patents, trademarks, trade secrets or other proprietary information (including unauthorized use of domain names); (e) make or contain fraudulent, deceptive, or misleading statements, claims, or representations (such as "phishing"); or (f) violate generally accepted standards of Internet usage;

2. Attempt to disrupt, degrade, impair or violate the integrity or security of the Services or Network or the computers, services, accounts, or networks of any other party (e.g., "hacking," "denial of service" attacks, etc.), including any activity that typically precedes attempts to breach security such as scanning, probing, or other testing or vulnerability assessment activity, or engaging in or permitting any network or hosting activity that results in the blacklisting or other blockage of Internet Protocol addresses assigned to Radiant.

3. View, modify, or tamper with files not owned by the Customer, unless the owner of such files has given Customer explicit permission to do so;

4. Transmit unsolicited bulk e-mail messages ("Spam"); receive replies from unsolicited emails; allow any computer attached to the Network to serve as a or configure any email server in such a way that it will accept third party emails for forwarding (e.g., "open mail relay"). Bulk email may only be sent to recipients who have expressly requested receipt of such e-mail messages via a "verified opt-in" process, which must be adhered to in its entirety for any bulk email to be considered "solicited" by Radiant. Users that send bulk email must maintain complete and accurate records of all e-mail subscription requests (verified opt-ins), specifically including the email and associated headers sent by every subscriber, and to immediately provide Radiant with such records upon request of Radiant. If a Customer has roaming End-Users who wish to use a common mail server that uses the Services or Network, that mail server must be configured to require user identification and authorization. Customers may not use a third-party provider to send Spam to promote a Web site hosted on or connected to the Services or Network. Customers and their End-Users shall not use the Services or Network in order to (a) send e-mail messages that are excessive and/or intended to harass or annoy others, (b) continue to send e-mail messages to a recipient that has indicated that he/she does not wish to receive them, (c) send e-mail with forged TCP/IP packet header information, or (d) send malicious e-mail;

5. Violate any charters, policies, rules or agreements promulgated by any search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, or other services accessed via the Services or Network ("Usenet Rules"), including, without limitation, any cross postings to unrelated news groups, continued posting of off-topic messages, and disrupting newsgroups with materials, postings, or activities that are inappropriate (as determined by Radiant in its sole discretion), unless such materials or activities are expressly allowed or encouraged under the Usenet Rules;

6. Violate the applicable acceptable use policies of other Internet Service Providers ("ISPs") when data, content, or other communications are carried across the networks of such ISPs.