ACCEPTABLE USE POLICY

These terms are subject to change from time to time. Please visit business.nrbn.ca for the most current Terms of Use.

1. By using NRBN's Internet Services and such other services provided by NRBN, its partners and associates, (collectively the "Supplier") you agree to the following terms of this Acceptable Use Policy. These terms and conditions are in addition to NRBN's applicable Terms of Service.
2. This Acceptable Use Policy ("AUP") constitutes the agreement between NRBN and you, subscribing to the Services. This Acceptable Use Policy governs your use of the Services and any devices and/or equipment used to support the Services including without limitation the modem and software which is provided to you and used in conjunction with the Services (the "Equipment"). By activating the Services, you expressly acknowledge that you have read, understand and agree to this Acceptable Use Policy and with NRBN's Terms of Service (collectively referred to as the "Agreement"). **If you do not wish to be bound by this Agreement, or any revisions made by NRBN, from time to time, do not activate or use the Services and contact NRBN.**
3. Use of the Services is subject to the following rules and guidelines. You are responsible for ensuring that the use of the Services complies with this Agreement.
4. The Service and Equipment that NRBN provides in connection with the Services are for consumer use and not to be used to operate a telecommunications service provider or advertising business.
5. It is prohibited for you to send unsolicited telecommunications that do not comply with anti-spam and Unsolicited Telecommunications Rules of the Canadian Radio-television and Telecommunications ("UTRs"), including the Canadian Anti Spam legislation known as CASL; or, in our sole judgment, cause significant disruption or elicit complaints from other users. The sending of bulk unsolicited commercial email, and the use of automated diallers to make unsolicited promotional voice calls, are examples of such prohibited use.

ILLEGAL ACTIVITY

6. NRBN prohibits the use of our Services for, and may interrupt, suspend or terminate your Services, if the Services are used to post, transmit, distribute, publish, disseminate, upload or download or otherwise make available in any way howsoever anything which:

- Harasses others in any way such as bullying, defaming, stalking, threatening or otherwise violating their legal rights;
    - Is abusive, profane, obscene, libellous, slanderous, advocates terrorist acts, fraudulent, deceptive or otherwise offensive or objectionable;
    - contains child pornographic material;

- contains a virus, lock, key, bomb, worm, cancelbot, Trojan horse or other harmful, limiting, debilitating, disruptive or destructive feature;
- contains, participates in, or incites or encourages hate speech,
- Is a criminal offence or gives rise to civil liability;
- is confidential to the party who originated the content;
- violates copyright or intellectual property rights. The customer assumes all risk regarding whether material is in the public domain;
- is a pyramid or other soliciting scheme;
- violates any municipal, provincial, federal or international law, order, rule or regulation, including those of the Canadian Radio-television and Telecommunication Commission applicable to the Services, NRBN or the Customer;

ELECTRONIC MAIL & MESSAGES

7. It is also a violation of this AUP to engage in any of the following activities:

- sending unsolicited e-mail (spamming), bulk or commercial messages. This includes but is not limited to bulk mailing of commercial advertising, charity requests, petitions for signatures, political and religious messages. Such messages may only be sent to those who have explicitly requested them, in accordance with CASL;

- forging or removing electronic mail headers or otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the Services or for any other purpose;

- sending messages that disrupt another Internet user's equipment, software, hardware or user display;

- sending large quantities of unwanted or unsolicited e-mail or VoIP messages (mail bombing or voicecasting);
- Sending multiple copies of the same or substantially similar messages, or sending very large messages to a recipient with the intent to disrupt a server or an account. The transmission of chain messages is prohibited.

SECURITY

8. It is strictly prohibited under this AUP to do or attempt to do the following:

- to invade another person's privacy; to appropriate or impersonate another person's identity (engage in "identity theft"); misrepresent or falsely state your relationship with another person or entity; unlawfully collect or store personal data about other persons or entities; or to forge any person's digital or manual signature; to forge, alter or obscure your identity (other than using a nickname) while using the Services;

- disrupt or otherwise interfere howsoever with the Supplier's network or the nodes or services thereof;
- gain unauthorized access to, alter or destroy any account, information or computer resource not belonging to the Customer (engage in "hacking", "spoofing", "phishing", "carding" or "pharming") by any means, device or tools (such as "packet sniffers") designed to facilitate the foregoing;
- disrupt the provision by the Supplier of any of its Services to any of its customers;
- disrupt computer networking telecommunications service to or from any Internet user, host, provider or network;
- improperly seizing or abusing operator privileges ("hacking");
- overloading a system or deliberately repeating actions in quick succession in order to fill the screens of other Internet users with text or other content (flooding);
- engage in broadcast attacks;
- attempting to "crash" a host;

• engage in counterfeit, fraudulent, subterfuge or malicious activities (splogging);
• unauthorized linking or framing or otherwise denying service ("denial of service attack") or otherwise denying, disrupting or misdirecting service to or use of service by any customer or end-user of the Supplier;

• using any device connected through the Services to maintain more than two simultaneous chat connections including, the use of automated programs such as "bots" or "clones". Automated programs may not be except when a representative of the Customer is physically present at the device;

• port scan a person's computer or wireless device without that person's consent, or use any tools designed to facilitate these scans;
• analyze or penetrate the Supplier's security mechanisms or do anything that may compromise the security of the Supplier' networks or systems in any way;

• use the Services to restrict, inhibit or otherwise interfere with the ability either of the Supplier to deliver or monitor the services provided by the Supplier or of any other person to use or enjoy the use of the products or services of the Supplier or the Internet;

• violating or circumventing any system or network security measures including engaging in unauthorized access or use of the Supplier's or a third party's network, data or information;

• use the Services for simultaneous sessions using the same User ID or password;

• alter, reproduce, or tamper with the Services or any function, component or identifier of Supplier's equipment;

9. Furthermore, it is strictly prohibited under this AUP to engage in any activity which the Supplier advises the Customer is, in the sole and unfettered discretion of the Supplier, similar to any of the foregoing or is reasonably and generally regarded in

the industry to be an unacceptable use of telecommunications services or is otherwise unacceptable use of the Services;

DETERMINATION BY SUPPLIER

10. The Customer accepts that the Supplier shall have the sole and unfettered right to decide if the Customer is in compliance with the requirements of this Acceptable Use Policy and the Customer unconditionally agrees that any decision by the Supplier in such regards shall be binding on the Customer until any such decision is proven to be incorrect.
11. The supplier is not responsible to forward email sent to any account that has been suspended or terminated. Such email may be returned to the sender, deleted or stored temporarily, at Supplier's sole discretion.

NO RESALE OR SHARING OF SERVICES WITHOUT PERMISSION

12. Unless permitted by the Service Agreement, sell, resell or make, directly or indirectly howsoever, any of the products or services received from the Supplier available to any third party.
13. If the Customer is at any time in breach of the requirements of this Acceptable Use Policy, the Customer agrees that the Supplier may immediately and without notice, and in addition to all other rights and remedies under the Service Agreement and at law and in equity, suspend the supply of any or all Services to the Customer pursuant to the Service Agreement. Any such suspension of the supply of the Services to the Customer shall not constitute a termination of the Service Agreement and shall not excuse the Customer from liability to make the payments to the Supplier required by the Service Agreement during the period that the provision of the Services to the Customer is suspended. The supply pursuant to the Service Agreement of any Services suspended pursuant to this Section shall resume upon the Customer no longer being in breach of any of the requirements of this Acceptable Use Policy and the Service Agreement and the payment by the Customer to the Supplier of any and all costs of the Supplier to suspend and restore service to the Customer and a $500 reinstitution charge. Breach of the requirements of this Acceptable Use Policy may result in termination of the Service Agreement pursuant to the Terms of Service comprising part of the Service Agreement.
14. In the event that any network with which the Supplier connects, directly or indirectly, or any regulatory or any industry oversight body of whatever nature or constitution advises of a system or use abuse originating with the Customer and as a consequence service to the Customer or to other customers of the Supplier or to the Supplier may be suspended then, regardless of whether or not the Customer is in fact the source of the advised abuse, the Customer agrees that the Supplier may immediately and without notice, and in addition to all other rights and remedies under the Service Agreement and at law and in equity, suspend the supply of the affected Services to the Customer pursuant to the Service Agreement. Any such suspension of the supply of the Services to the Customer shall not constitute a termination of the Service Agreement and shall not excuse the Customer from liability to make the payments to the Supplier required by the Service Agreement

during the period that the provision of the Services to the Customer is suspended. The supply of Services pursuant to the Service Agreement of any Services suspended pursuant to this Section shall resume upon the Customer no longer being or being regarded as the source of the advised abuse. If the Customer was not the source of the advised abuse, then the resumption of the provision of the Services to the Customer shall be made without any charge therefor by the Supplier to the Customer and the Supplier will not charge the Customer for the suspended Services for the period of suspension. If the Customer was the source of the advised abuse, then the resumption of the provision of the Services to the Customer shall be conditional upon the payment by the Customer to the Supplier of any and all costs of the Supplier to suspend and restore service to the Customer and a $500 reinstitution charge. If the Customer is the source of the advised abuse, then the Supplier may terminate the Service Agreement pursuant to the Terms of Service comprising part of the Service Agreement.

INTERNET TRAFFIC MANAGEMENT POLICIES ("IMTPs")

15. NRBN may in its sole discretion, use reasonable traffic management policies to ensure equitable access to its network for all of NRBN's Internet customers. NRBN may employ IMTPs, in the event of significant network congestion due to network failure, a force majeure event, or other transport network constraint that impacts its customers' use of the Internet. IMTPs are not intended to impact customers' activities such as on-line banking, on-line shopping, or the use of VoIP services. In most cases, the customer experience should not be affected by the employment of Internet Traffic Management Policies.

16. NRBN does not routinely monitor the activity of its customers for violation of this AUP. However, NRBN may take action in the event that it becomes aware of suspected AUP violations. NRBN may monitor bandwidth usage and other metrics in order to identify AUP violations and to protect its network and its customers.

17. In the course of investigation of AUP violations, NRBN may suspend the account of a customer, which violates the AUP, and may delete from its servers, any material which violates the AUP.

LAW ENFORCEMENT REQUIREMENTS

18. NRBN may be required to cooperate with law enforcement officials, in the investigation of criminal activity. You hereby acknowledge that NRBN may cooperate with law enforcement authorities in the investigation of suspected criminal activity, and/or system administrators at other Internet Service Providers or network operators, in order to enforce this AUP. Such cooperation may include but is not limited to the provision of the username, IP address or other identifying information about a customer, in accordance with the guidelines set out in NRBN's Privacy Policy.