

ACCEPTABLE USE POLICY (INTERNET)

This Acceptable Use Policy (AUP) is an integral part of the provision of Our ISP services. If You engage in any of the activities prohibited by this AUP document We may suspend or terminate Your account. It is designed to help protect Us, Our customers and the Internet community in general from irresponsible or, in some cases, illegal activities.

Prohibited Uses of Our Internet access connections:

- 1.1. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
- 1.2. Sending unsolicited bulk email ("spam"). The sending of any form of spam through Our servers is prohibited. Likewise, the sending of spam from another service provider advertising a web site, email address or utilizing any resource hosted on IntraLAN's servers, is prohibited. IntraLAN accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another Internet Service Provider where those messages violate this Policy or that of the other provider.
- 1.3. Running Unconfirmed Mailing Lists. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by IntraLAN customers must be Closed-loop ("Confirmed Opt-in"). The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list. Purchasing lists of email addresses from 3rd parties for mailing to from any IntraLAN-hosted domain, or referencing any IntraLAN account, is prohibited.
- 1.4. Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to send Unsolicited Bulk Email, initiation of ping, flooding, mail-bombing, denial of service attacks.
- 1.5. Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org.
- 1.6. Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g., "cracking").
- 1.7. Obtaining or attempting to obtain service by any means or device with intent to avoid payment.
- 1.8. Unauthorized access, alteration, destruction, or any attempt thereof, of any information of any IntraLAN customers or end-users by any means or device.
- 1.9. Knowingly engage in any activities designed to harass, or that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any other user whether on the IntraLAN network or on another provider's network.