

BreedeneNet Acceptable Use Policy

In this Policy:

- “the service provider” means BreedeneNet CC, CK 2005/091092/23
- “the service” means the internet access package and related services such as hosting and mailbox provision as requested and agreed upon by the customer and provided by the service provider;
- “infrastructure” means all facilities, equipment, software and other amenities owned or leased by the service provider and utilised in or related to the provision of the service

1. Introduction

1.1 This Acceptable Use Policy ("AUP") specifies the types of actions and specific actions prohibited to users of the network and systems ("infrastructure") of BreedeneNet ("the service provider"), and is intended to enhance the use of the Internet by preventing unacceptable use. Users are required to adhere to all the policies specified in this AUP without exception.

1.2 This AUP forms part of and is incorporated by reference into the Terms and Conditions governing the provision of the service. An updated copy hereof will be available at <http://www.breedene.co.za/files/terms.PDF>

1.3 This AUP may be amended from time to time as required by legal developments. While the service provider will take steps to notify users of amendments users retain the sole responsibility for acquainting themselves with such amendments and will be regarded as having agreed thereto through continued use of the service.

2. Compliance with applicable laws and regulations

2.1 The service provider's infrastructure and the service provided may be used only for lawful purposes. Users may not violate any applicable laws or regulations of South Africa within the territory of South Africa.

2.2 Transmission, distribution or storage of any material on or through the infrastructure 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 authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

3. Transmission of data

- 3.1 The user acknowledges that the service provider is unable to exercise control over the content of the information passing over the infrastructure and the Internet, including any websites, electronic mail transmissions, news groups or other material and associated materials such as traffic data created or accessible over its infrastructure. The service provider is not responsible for the content of any messages or other information transmitted over its infrastructure.
- 3.2 The user acknowledges further that the service provider is under no general obligation to monitor traffic passing over the infrastructure and the Internet.

4. System and Network Security

- 4.1 Any reference to systems and networks under this section includes the Internet (and all those systems and/or networks to which user is granted access through the service provided) and includes but is not limited to the infrastructure of the service provider. The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").
- 4.2 Violations of system or network security by the user are prohibited, and may result in civil or criminal liability. The service provider will investigate incidents involving such violations and will involve and cooperate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:
 - 4.2.1 Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures;
 - 4.2.2 Unauthorised monitoring of data or traffic on the network or systems;
 - 4.2.3 Interference with service to any user, host or network including, without limitation, mail-bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
 - 4.2.4 Forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

5. Disclaimer and indemnity

- 5.1 The service provider disclaims all and any liability for any claim or action or other legal proceeding, howsoever arising, from unacceptable use or use in contravention of this AUP of the service or the service provider's infrastructure by users, including special and consequential damages and damages for loss of profits and pure economic loss.
- 5.2 The user agrees to indemnify and hold the service provider harmless in respect of liability for any claim or action or other legal proceeding, howsoever arising, from unacceptable use or use in contravention of this AUP or of the service or the service provider's infrastructure by users, including special and consequential damages and damages for loss of profits and pure economic loss.

6. E-mail Use

- 6.1 It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements, etc). This is strongly objected to by most Internet users and the repercussions against the offending party and the service provider and can often result in disruption of service to other users.
- 6.2 Users' attention is drawn to section 45 of the Electronic Communications and Transactions Act No. 25 of 2002 (Republic of South Africa) and the fact that failure to comply with the provisions of section 45 can result in criminal liability.
- 6.3 Maintaining of mailing lists by users of the service is acceptable only when done with the written permission and approval of the list members, and at the members' sole discretion. Should mailing lists contain invalid or undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed.
- 6.4 The service provider reserves the right to request that a user provide documentary evidence of the written permission or approval obtained by the user in respect of any complaining third party or parties and users consent to delivering such material within 48 hours of receipt of a written request from the service provider to this effect. Failure to respond timeously to such a request will constitute grounds for termination or suspension of the user's account or such other sanction as may be proportionate in the circumstances.

7. Public relay

- 7.1 Public relay occurs when a mail server is accessed by a third party from another domain and utilised to deliver mails, without the authority or consent of the owner of the mailserv. Users' mail servers must be secure against public relay as a protection to both themselves and the Internet at large. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed.
- 7.2 The service provider reserves the right to examine users' mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the user. The service provider also reserves the right to examine the mail servers of any users using mail servers provided by the service provider for "smarthosting" (when the user relays its mail off a service provider mail server to a mail server of its own) or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be done in a manner aimed at preserving customer privacy.
- 7.3 Notwithstanding measures taken by the service provider in this regard users acknowledge that the responsibility for taking reasonable measures to secure their mail servers against public relay remains solely that of the user and the service provider will accept no liability in this regard (unless arising from its own negligence in the securing of mail servers owned by it).

8. Interception and Monitoring

- 8.1 Users expressly acknowledge the fact of and consent to the lawful monitoring and interception of traffic carried over the service provider's infrastructure by the service provider or related entities under the following circumstances:
- 8.1.1 Where required under the provisions of the Interception and Monitoring Prohibition Act No 127 of 1992 or the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 or any other law;
 - 8.1.2 Where required by court order;
 - 8.1.3 Where required for the maintenance of system and network integrity and security;
 - 8.1.4 Where required for the efficient provision of services, including billing and bandwidth and performance monitoring;
 - 8.1.5 Where required for the actioning of a takedown notice or complaint in terms of this AUP.
- 8.2 The service provider will undertake interception and monitoring in accordance with the following principles:
- 8.2.1 The privacy of users is a fundamental right and any interception and monitoring will accordingly be reasonable and proportionate according to the circumstances;
 - 8.2.2 The actual content of any private communication will not be accessed unless required by law or otherwise regarded as necessary for the achievements of one or more of the objectives set out above;
 - 8.2.3 Staff and specifically contracted entities will be bound by confidentiality agreements in respect of interception and monitoring activities.

9. Take Down Notices

- 9.1 The procedure in respect of take-down notifications is laid out in section 77 of the Electronic Communications and Transactions Act No. 25 of 2002 ("ECT Act").
- 9.2 The essence of the procedure is that a complainant who believes that an ISP is providing services which infringe his or her rights may issue a notification to the ISP or its designated agent, requesting that such services be terminated.
- 9.3 Under section 77 of the ECT Act a take-down notice must contain the following information:
- 9.2.1 the full names and address of the complainant;
 - 9.2.2 the written or electronic signature of the complainant;
 - 9.2.3 identification of the right that has allegedly been infringed;
 - 9.2.4 identification of the material or activity that is claimed to be the subject of unlawful activity;
 - 9.2.5 the remedial action required to be taken by the service provider in respect of the complaint;
 - 9.2.6 telephonic and electronic contact details, if any, of the complainant;
 - 9.2.7 a statement that the complainant is acting in good faith; and

9.2.8 a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct.

9.4 Take down notices should be sent to complaints@ispa.org.za

9.5 The service provider will take such steps as are available to alert any affected user of the receipt of a takedown notice but is under no obligation to do so. Users acknowledge and agree that they will co-operate fully with the service provider where it is required by a validly-issued take down notice to remove content or disable access to content.

9.6 Users are encouraged to voluntarily remove any content which is the subject of a takedown notice.

10. Complaints / Failure to observe this AUP

10.1 Upon receipt of a complaint, or having become aware of an incident, the service provider reserves the right to, as may be applicable:

10.2.1 Inform the user's network administrator of the incident and require the network administrator or network owner to deal with the incident according to this AUP.

10.2.2 In the case of individual users suspend the user's account and withdraw the user's network access privileges completely.

10.2.3 Charge the offending parties for administrative costs as well as for machine and human time lost due to the incident.

10.2.4 In severe cases suspend access of the user's entire network until abuse can be prevented by appropriate means.

10.2.5 Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies.

10.2 The service provider reserves the right to take any one or more of the steps listed above, insofar as it deems them proportionate, in its absolute and sole discretion, against the offending party.

10.3 All cases of violation of the above Acceptable Use Policy should be reported to abuse@breede.co.za