interoute

from the ground to the cloud

ACCEPTABLE USE POLICY

CONTENTS

1 GENERAL

Interoute reserves the right to modify the Acceptable Use Policy ("AUP") from time to time. Changes to this Acceptable Use Policy will be notified to Customer in accordance with the terms and conditions of our agreement with the Customer.

Interoute aims to promote a high level of responsible behaviour in connection with the use of the Internet, the Interoute Network and the Interoute services, systems, websites and products including but not limited to those services that utilize or provide access to the Interoute Network, any other network (including the PSTN) and/or the Internet (the "Services") and for this purpose has created this Acceptable Use Policy, inter alia, to:

- define acceptable practices for the use of any of the Services;
- protect the interests and reputations, and resources of Interoute and its Customers;
- protect, as far as Interoute is reasonably able to do, the Internet community as a whole from the improper and/or illegal or criminal behaviour;
- Protect Interoute and its Customers from any third party claims alleging that the use of the Interoute Network or the Services is inappropriate or creates damage to such third party.

All Customers of Interoute must read and comply with this Acceptable Use Policy and, where such Customers provide services to their own users (e.g. resellers or downstream service providers), take all reasonable steps to ensure that their own users are aware of and comply with this Acceptable Use Policy or an acceptable use policy with terms the same or substantially similar to this Acceptable Use Policy, including, where necessary, terminating access for any such users who do not comply with the Acceptable Use Policy. Where the context requires references to "Customer" in this Acceptable Use Policy will be deemed to include the Customer's users or customers.

All Customers of Interoute are responsible for violations of this AUP by anyone using the Customer's services with the Customer's permission or on an unauthorized basis as a result of the Customer's failure to use reasonable security precautions. Customer use of the Services to assist another person in an activity that would violate this AUP if performed by Customer is a violation of the AUP.

By using any of the Services, a Customer acknowledges that it has read, understood and agrees to comply with the Acceptable Use Policy. Customers must also ensure that the terms under which they provide services to their own users require that each such user acknowledges that they have read, understood and agreed to abide by this Acceptable Use Policy or an acceptable use policy with terms the same or substantially similar to this Acceptable Use Policy,. Breaches of the Acceptable Use Policy by a user who obtains access via a Customer (e.g. resellers or downstream service providers) will also be considered to be a breach of the Acceptable Use Policy by that Customer.

Each Customer must report to Interoute by e-mail to abuse@interoute.com any violations of the Acceptable Use Policy promptly after first becoming aware of such violation and shall provide all reasonable assistance to Interoute to investigate and resolve any reported claims, complaints and/or problems arising out of the Services.

Customers must immediately report to Interoute by e-mail to abuse@interoute.com any network issue that might compromise the stability, continuity or security of the Services. Customers must co-operate with Interoute and any properly authorised law enforcement or regulatory authority or body to investigate claims of criminal, illegal or other inappropriate behaviour.

Any complaints or enquiries regarding any breach of the Acceptable Use Policy should be sent by e-mail to abuse@interoute.com.

2 DISCLAIMER

While Interoute reserves the right to suspend or terminate the Services or the Customer's access thereto, edit or remove any content that it deems to be in breach of the Acceptable Use Policy or is otherwise harmful or offensive, Interoute does not intend to review, monitor or control content sent or received by Customers using the Services unless required by law and accordingly Interoute accepts no responsibility or liability to Customers or any other person for the content of any communications that are transmitted by or made available to Customers or their users, regardless of whether they originated from the Interoute Network or the Services.

In no event shall Interoute be liable to any user of its Services (Customer or end user) nor any third party for any direct, indirect, special or consequential damages for actions taken pursuant to this AUP, including, but not limited to, any lost profits, business interruption, loss of programs or other data, or otherwise.

3 RIGHTS OF INTEROUTE IN CASE OF VIOLATION OF THIS AUP

3.1 Suspension or termination

If Customers or their users engage in conduct which is in violation of the Acceptable Use Policy or is otherwise illegal or improper, Interoute reserves the **right to suspend and/or terminate** any Service(s) or the Customer's access to the Service. Where practicable, Interoute will attempt to notify the Customer of any activity that breaches this Acceptable Use Policy and request that the Customer or its user ceases such activity. However, where any activity of a Customer threatens the integrity or viability of the Interoute Network or the Services or involves illegal acts, fraud, unauthorised access/interference, spamming/mail bombing, e-mail relaying, alteration of the Customer's source IP address information, harassment, copyright infringement, the introduction of malicious programs or interference with Interoute's monitoring, Interoute reserves the right to suspend any Service or a Customer's access to any Service without notice.

In addition, Interoute reserves the right to take appropriate action, legal or otherwise, including cooperation with authorities, against any Customer or other person responsible for the violation of the Acceptable Use Policy.

Interoute may require the Customer to help in resolving a security incident where that Customer system(s) may have been involved.

3.2 Implementation of technical mechanisms to prevent violation

Interoute reserves the right, where feasible, to implement technical mechanisms to prevent any violation of the Acceptable Use Policy.

3.3 Costs associated with dealing with the breach

In addition, Interoute reserves the right to charge the Customer to cover administrative costs associated with the time and resources used to deal with the breach of this AUP by the Customer including, but not limited to, recovery of the costs of identifying offenders and removing them from or discontinuing providing them the Services.

4 PROHIBITED USE

The Customer must not engage in any activity whether lawful or unlawful which is detrimental to Interoute's operations, reputation, goodwill or customers. The following are non-exclusive examples of use that is strictly prohibited under the Acceptable Use Policy and are provided merely as guidelines:

4.1 Illegal Activity

Customers must only use the Services for lawful purposes and must not use the Services for any purpose which breaches any applicable law, regulation, treaty or tariff. This includes, without limitation, the use, transmission or storing on Interoute network or Interoute physical or virtual servers of any data or material protected by copyright, trademark, trade secret, patent, or other intellectual property right without proper authorisation, and/or the transmission of any material which constitutes an illegal threat, violates applicable import and export laws (including the transmission of encryption software), is obscene, indecent, defamatory or otherwise in violation of any applicable law including, but not limited to, financial services, consumer protection, unfair competition, antidiscrimination, or false advertising. Without limitation, illegal activity will also include defamation, obscenity, child pornography or software piracy.

Customer may not use the Services to engage in any conduct that is likely to result in retaliation against Interoute Services., Interoute or Interoute's employees, officers or agents, including engaging in behaviour that results in any server being the target of a distributed denial of service attack (DDoS); or Any action which directly or indirectly results in any of our IP space being listed on any abuse database (i.e. Spamhaus).

4.2 Harassment

Customers must not use the Services to harass any person, whether by language, frequency or size of e-mail. Continuing to send any e-mail after being asked to stop will generally be considered harassment and harassment may take any recognised form and will include, but not be limited to, harassment according to race, nationality, religion, sex, sexual persuasion, political affiliation, trade union membership, physical or mental appearance or state or any other form of harassment.

4.3 Violation of Other Applicable Acceptable Use Policies

Customers must not breach the applicable acceptable use policies of any other networks, machines or services which are accessed by or through the Services.

4.4 Vulnerability Testing/Unauthorised Access/Interference

Customers must not attempt to probe, scan, penetrate or test the vulnerability of Interoute's Services, or to breach Interoute's security or authentication measures, whether by passive or intrusive techniques or gain unauthorised access to, or attempt to interfere with or compromise the normal functioning, operation or security of neither the Services or the Interoute network, nor any network, systems, machines or services without agreeing to and complying with the current Interoute Penetration Test Agreement.

Customers must not use the Services or the Interoute Network to compromise or deny any third party access the Services or the Internet.

A Customer may not use the Services to monitor any data, information or communications without proper authorisation. Customers must not attempt to gain unauthorised access to the user accounts or passwords of other users, or otherwise violate the privacy of any other Customers or users. Customers must not attempt to intercept, redirect or otherwise interfere with communications intended for another person.

4.5 Fraud, phishing, pharming

Customers must not attempt to impersonate another person by altering source IP information or sending e-mail messages with a false header or other user identification information. Customers must not attempt to fraudulently conceal, forge or otherwise falsify their or another person's identity in connection with the use of the Services.

4.6 E-mail relay, spoofing and forging

Any use of another person's e-mail server to relay e-mail or any other messages (including Instant Messaging) without express authorisation from such person is prohibited.

Falsifying user or other Service related information, including, but not limited to, intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return mailing and Internet protocol addresses, provided to Interoute or to other Service users or engaging in any activities or actions intended to withhold or cloak Customer's or its end users identity or contact information is prohibited.

4.7 Open mail relays

Customer may not maintain an open mail relay. A failure to take appropriate steps to close an open mail relay shall entitle Interoute to suspend or terminate Services.

4.8 Electronic Communications

Customer may not distribute, publish, or send through the Services: (1) unsolicited advertisements, solicitations, commercial e-mail messages or promotional messages of any kind (commonly referred to as "spam"); (2) unsolicited informational announcements; (3) chain mail; (4) numerous copies of the same or substantially similar messages; (5) empty messages; (6) messages which contain no substantive content; or (7) very large messages or files that disrupt a server, account, newsgroup, or chat service.

Likewise, you may not (1) participate in collecting e-mail addresses, screen names, or other identifiers of others (without Company's prior written consent), a practice sometimes known as spidering or harvesting; (2) participate in using software (including "spyware") designed to facilitate such activity; (3) collect responses from unsolicited messages; or (4) use any of our mail servers or another site's mail server to relay mail without the express permission of the account holder or the site. Customer will not access any Usenet newsgroups via any other network. Without notice to you and at any time, we may add, remove, or modify Usenet newsgroups or services and may modify or restrict the bandwidth available to download content from Usenet newsgroups.

4.9 Postings

All postings to USENET groups, websites, forums, online communities and groups must be in accordance with that group's charter and other applicable policies. Customers must not cross post to unrelated news groups or news groups where such posting would breach any applicable charter or policy.

4.10 Malicious Programs

Customers must not intentionally or recklessly introduce malicious programs onto the Services, the Interoute Network or the Internet including, but not limited to, computer viruses, spyware, malware, spamware, corrupted data, worms, Trojan Horses etc.

Customers must not distribute software that covertly gathers or transmits information about a user;

Customers must not distribute advertisement delivery software unless: (i) the End user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software, and (ii) the software is easily removable by use of standard tools for such purpose included on major operating systems (such as Microsoft's "add/remove" tool);

4.11 Unauthorised monitoring, scanning, or intercepting

Customers must not monitor or scan the networks of others, or the use by other persons of the Services or any other services without proper authorisation. Customers must not intercept messages or access data for which the Customer is not the intended recipient or log into a server account of another Customer without proper authorisation.

Customer shall respect all applicable laws concerning the privacy of online communications.

4.12 Provision of false information

Customers must not provide false or incorrect information or data to Interoute when signing up for any Services. Interoute reserves the right to suspend or terminate any Service where false or incorrect information or data has been provided.

4.13 No High Risk Use

Customer may not use the Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage. Customer must inform Interoute if Customer intends to use, the Services in connection with aircraft or other modes of human mass transportation or nuclear or chemical facilities.

4.14 Interference with Interoute's monitoring

Customers must not attempt to circumvent or distort the procedures or processes that Interoute uses to measure time, bandwidth use, availability, health or other utilization of the Services.

4.15 Excessive Usage

If Interoute has reserved specific bandwidth limitations and/or burst and/or other usage for a Customer in accordance with a Customer's request, that Customer's use of the Service shall not be in excess of those limitations.

4.16 Password Protection and Transfer of Account

Customers are responsible for protecting the confidentiality of their password and user account numbers and may not share either their password or user account number with any other person. Customers may not transfer their account to anyone without the prior written account of Interoute.

Customers must report to Interoute by e-mail to Global.Noc@interoute.com any loss of their password or any other situation in which they believe the security of their password may have been compromised promptly after first becoming aware of such loss or other situation.

4.17 Copyright

Customers must only use the Services in accordance with all applicable intellectual property laws. Interoute reserve the right to remove or disable any material it has reason to believe infringes applicable Intellectual Property laws.

Customers must only use the Services respecting all applicable Intellectual Property Rights of any third party. Interoute shall reserves the right to remove or disable any material it has reason to believe infringes any third party Intellectual Property Rights.

For the avoidance of doubt, Interoute does not accept any responsibility or liability to owners or other users of any Intellectual Property Rights, for the acts and/or omissions of Customers in connection with or related to the Services in respect of any Intellectual Property Rights.

Customers must use the Services in accordance with the generally accepted norms and expectations of the Internet community in force.

Customer may not (and Customer may not permit anyone else to) copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of any Software or programme provided by Interoute as part of its Services any part thereof, unless this is expressly permitted or required by law, or unless specifically authorised by Interoute in writing.

5 CUSTOMER INCIDENTS

When Customer is a victim of an event that would be considered as prohibited use had the Customer been the instigator of such event, Interoute reserves the right to act as per clause 3 of this AUP.