

# Acceptable Use Policy

## 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 and the Interoute Network and for this purpose has created this Acceptable Use Policy, inter alia, to:

- define acceptable practices for the use of any of Interoute's services that provide access to the Interoute Network, any other network (including the PSTN) and/or the Internet ("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.

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.

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](mailto: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](mailto: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](mailto:abuse@interoute.com).

## **2. Disclaimer**

While Interoute reserves the right to 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.

## **3. Rights of Interoute**

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 the Service 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 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 Network 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, against any Customer or other person responsible for the violation of the Acceptable Use Policy.

Interoute reserves the right to, where feasible, implement technical mechanisms to prevent any violation of the Acceptable Use Policy. In addition, Interoute reserves the right to charge the Customer to cover administrative costs

associated with the prohibited activities of the Customer including, but not limited to, recovery of the costs of identifying offenders and removing them from or discontinuing providing them Service, in an amount (i) equal to Interoute actual expenses incurred in preventing or responding to such activity, or (ii) up to EUR 10000, whichever is greater.

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.

#### **4. Prohibited Use**

The following are non-exclusive examples of use that is strictly prohibited under the Acceptable Use Policy and are provided merely as guidelines:

##### ***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 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 unlawful because 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.

##### ***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.

##### ***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.

##### ***Unauthorised Access/Interference***

Customers must not attempt to gain unauthorised access to, or attempt to interfere with or compromise the normal functioning, operation or security with any network, machines or services. Customers must not use the Services 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.

### ***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.

### ***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.

### ***Open mail relays***

The operation of an open mail relay may be vulnerable to senders of mass unsolicited e-mail hijacking the server for spamming. A failure to take appropriate steps to close an open mail relay shall entitle Interoute to suspend or terminate Services.

### ***Spamming/Mail bombing***

Customers may not use the Services to transmit excessive amounts of unsolicited commercial e-mail messages or send excessive attachments to another user. Use of the Services to send or receive responses to unsolicited commercial e-mails or series of unsolicited commercial e-mails or large attachments sent to one user is prohibited. This shall include, but not be limited to, the collection of e-mail addresses for the purposes of sending excessive amounts of unsolicited e-mail.

### ***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.

### ***Malicious Programs***

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

### ***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.

### ***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.

### ***Interference with Interoute's Network Monitoring***

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

### ***Excessive Usage***

If Interoute has reserved specific bandwidth limitations 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.

### ***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](mailto: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.

***Copyright***

Customers must only use the Services in accordance with all applicable intellectual property laws. Interoute reserves 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 from time to time.

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.