Business Services

1 ACCEPTABLE USE POLICY FOR ORANGE PRODUCTS & SERVICES

Orange Business Services ("Orange") will not be responsible or liable for any data, information or communications obtained or transmitted using Orange's products, services, networks, systems and web sites (collectively, "Orange Services") or for any consequences or damages suffered by Customer, its Users or any other user arising out of or relating thereto. Although Orange does not pre-screen content of communications and information received, sent, or stored using the Orange Services, Orange and its designees will have the right (but not the obligation), in their sole discretion, to block, delete, move or refuse to transmit any data that is made available via such Orange Services, including any data that violates the terms of this Acceptable Use Policy ("Policy") or Customer's agreement with Orange, or that is otherwise reasonably objectionable. Customer agrees that it will evaluate, and bear all risks associated with, the receipt, transmission, and use of any content. Customer also will use, and will ensure that its Users use, the Orange Services only in compliance with the terms and conditions set forth in the relevant Service Description(s). By using the Orange Services, Customer agrees that it has read, understood and agrees to be bound by the terms of this AUP.

Customer agrees that it and its Users will not, and that they will not permit or assist others to, abuse or fraudulently use Orange's products or services, whether directly or indirectly, including but not limited to the following:

(a) Impersonating any person or entity (e.g. an Orange employee or officer), falsely stating or otherwise misrepresenting an affiliation with a person or entity, or forging headers or otherwise manipulating identifiers to disguise the origin of any content transmitted through the service;

(b) Sending or posting any unsolicited e-mail to any Usenet or other newsgroup, forum, e-mail mailing list or other similar group list that causes complaints from the recipients of such unsolicited e-mail;

(c) Mail-bombing or spamming (i.e. the act of sending a large number of unsolicited e-mail messages within a short period of time to one or more individual e-mail accounts) or sending one unsolicited e-mail message to ten or more individual e-mail users, where the message could reasonably be expected to cause complaints from some of the recipients;

(d) E-mailing or otherwise transmitting any material that contains software viruses, Trojan horses, or any other computer code, files or programs designed or intended to interrupt, destroy, invade, gain unauthorized access to, corrupt, observe, limit the functionality of, or modify without authorization, data, software, computing or network devices or telecommunications equipment;

(e) Transmitting, distributing, disseminating, publishing or storing any material that (i) is in violation of any applicable law, rule or regulation, including any law or regulation regarding privacy or wire fraud, or (ii) is defamatory, abusive, obscene, indecent, false, or harassing; or (iii) threatens or encourages bodily harm, destruction of property, or infringement or misappropriation of the lawful rights of any party, including any Intellectual Property Rights;

(f) E-mailing or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright, right of publicity or other proprietary right of any party, or any information that the sender does not have a right to transmit under any law or under contractual or fiduciary relationships (e.g. inside information, trade secrets, proprietary and/or confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements);

(g) Attempting to gain unauthorized access to any account or computer resource not belonging to the user;

(h) Obtaining or attempting to obtain service by any means or device with intent to avoid payment;

(i) Unauthorized accessing, altering, interfering with, or destruction of any network, system, equipment or information by any means or device, or any attempt to do any of the foregoing, including any attempt to (i) retrieve, alter or destroy data, (ii) probe, scan or test the vulnerability of a system or network, or (iii) breach or defeat system or network security, authentication, authorization, confidentiality, intrusion detection, monitoring, or other security measures;

(j) Knowingly engaging in any activity that will result in degradation of service (e.g. synchronized attacks) to any Orange customer or a member of the Internet community;

(k) Changing, modifying, deleting or disabling any IP addresses or passwords set up by Orange, without Orange's prior written consent;

(l) Using the Orange products or services to interfere with the use of Orange's network by other customers or authorized users (e.g. attempting to intercept, redirect or otherwise interfere with communications intended for others), or in violation of the law or in aid of any unlawful act.

Orange explicitly prohibits the sending of unsolicited commercial email (UCE) and unsolicited bulk email (UBE), including without limitation, commercial advertising and informational announcements.

Activities that facilitate UCE or UBE are prohibited. Using another's site mail server to relay mail without the express authorization of the site owner is prohibited.

In the event of any activity that violates this Policy, Orange may, without notice, terminate the relevant products or services or take such other actions as it reasonably deems appropriate with respect to the applicable products or services without notice. Orange will not issue a service credit for any outages that may arise out of or relate to any Policy violations.

Orange will investigate incidents involving alleged Policy violations, which may include monitoring usage, and may cooperate with legal authorities and/or third parties in case of any suspected criminal violation.

Customer will report all Policy violations to the Security Operations Center at global.security.org@orange.com or such other email address as may be provided by Orange from time to time, and provide the following information:

- The IP address(es) involved the violation.
- The date and time of the violation, including the time zone or offset from UTC.
- Evidence of the violation (e.g. excerpts of syslog files).

Customer agrees that will comply with, and will require its Users to comply with, any other usage policies of Orange's suppliers that apply to the products and services. Orange reserves the right to modify this Policy at any time. Any use of the Orange Services following such modifications will constitute acceptance of the Policy as modified.

END OF ACCEPTABLE USE POLICY FOR ORANGE PRODUCTS & SERVICES