

Acceptable Use Policy (AUP)

1 Scope and Application of the AUP

1.1 This acceptable use policy applies to all customers of IP and Internet services provided by T-Systems, and forms an integrated part of the contractual relationship between T-Systems and the customer.

1.2 This policy lays down rules for the acceptable use of the IP and Internet services provided by T-Systems.

2 Changes to the AUP

2.1 T-Systems reserves the right to make changes to this AUP at any time. Such changes will be published on the Internet at www.t-systems.ch, and individual customers will also be notified directly when appropriate.

3 Acknowledgement of Awareness and Obligations of the Customer

3.1 The customer acknowledges that it is aware of the possibility that the content and product information it disseminates may have a negative impact on the reputation and business of T-Systems and its customers. Accordingly, the customer is under a strict obligation to observe the rules given in this document and to abide by the rules of conduct known to Internet users as "netiquette".

3.2 T-Systems services may be used solely in accordance with current international and Swiss law and other regulations. Such regulations include in particular the "Requests for Comment" (RFCs) of the Internet Society (ISOC) and any applicable "Memorandums of Understanding" of the International Telecommunication Union (ITU). The customer shall also observe the principles of fairness and clarity, and shall refrain from any behaviour or conduct of business that is deceptive, misleading or contrary to good faith.

3.3 The customer shall also take suitable and reasonable measures against wrongful access to its systems and their wrongful use.

4 Misuse for the Purposes of the AUP

4.1 The misuse of IP and Internet services is forbidden. Misuse for the purposes of this AUP refers in particular, but not exclusively, to the following:

- 4.1.1 unauthorised access or tentative of unauthorised access to data, systems or external networks;
- 4.1.2 passive or non-interventionist techniques such as the scanning or probing of other parties' networks (e.g. checking other parties' computers for particular services or their vulnerability) using portscans;
- 4.1.3 sniffing, i.e. monitoring and analysing other parties' network traffic;
- 4.1.4 flooding, i.e. deliberately overloading other parties' systems or networks with a view to impairing their operation or making their operation impossible (Denial of Service);
- 4.1.5 spoofing, i.e. falsifying network packets, particularly of TCP/IP header information;

4.1.6 dispatching unwanted commercial advertising using the following media:

- personal e-mails
- SMS (Short Message Service)
- e-mail lists
- Usenet discussion groups;

4.1.7 sending chain-mails according to the "snowball" principle, i.e. sending e-mail messages and asking for them to be forwarded to the largest possible number of other recipients;

4.1.8 mail spamming, i.e. sending unsolicited commercial e-mail messages (UCE) or unsolicited bulk e-mail (UBE);

4.1.9 sending e-mails with content designed to annoy;

4.1.10 mail bombing, i.e. sending a large number of e-mail messages to the same recipient;

4.1.11 unauthorised use of another party's mail server as a relay without prior consent from its owner;

4.1.12 excessive multi-posting (EMP), i.e. sending the same or almost the same Usenet message in large numbers;

4.1.13 excessive cross-posting (ECP), i.e. simultaneously sending a Usenet message to a large number of news groups;

4.1.14 SMS spamming, i.e. flooding mailboxes, Usenet groups or other on-line forums with messages which are pointless, unrequested or otherwise annoying;

4.1.15 damaging or impairing of T-Systems' equipment, hardware, software, data or operations.

5 Illegal Material and criminal Acts

5.1 The customer is responsible for ensuring that the use of the services sourced from T-Systems by the customer or associated users (employees, family members, end customers, etc) complies with the relevant legal provisions, particularly regarding data protection, telecommunications law, copyright law and anti-money laundering law. The customer furthermore undertakes not to use the services made available to it for either committing or assisting in any criminal acts.

5.2 The content of the IP traffic of a T-Systems customer, either from or to its location, must not breach the requirements of local laws, as for example in the case of unauthorised games of chance, representations of violence, pornography, incitement to criminal activity or violence, or racial discrimination. Where access to certain content is restricted to certain persons, the customer is required to take appropriate steps to ensure that unauthorised persons do not gain access to the material in question (e.g. children accessing pornography). Where certain activities or Internet contents are not expressly prohibited by local laws, T-Systems itself prohibits the use of its services for activities which exploit minors, illegally sell copyright protected or licensed material, or insult, degrade or annoy persons or groups on the basis of their race or ethnicity.

5.3 The customer may not use IP or Internet services of T-Systems in order to offer, sell or advertise goods or services if and to the extent such activities are forbidden or restricted under local law. Insofar financial transactions are carried out using IP or Internet services of T-Systems, the customer shall comply with all applicable regulations, in particular obligations of due diligence regarding the verification of the identity of the contracting party and the origin of valuables.

6 Provocation of Network Attacks

6.1 The display of any content causing an excessively high level of network traffic, and hence jeopardising the security of T-Systems' computer systems, by deliberately provoking network attacks from the Internet (e.g. pornographic content, statements by extreme political or religious groups, etc) is prohibited. This also includes publications able to have a negative impact on the image or business of T-Systems or its customers. T-Systems reserves the right to remove such content without prior notice, and, if appropriate, to block network access.

7 Reporting Cases of Misuse to T-Systems

If the customer identifies a case of the misuse of services, equipment or software - in particular use by a third party in breach of law or a contract -, it is required to notify T-Systems accordingly.

7.1 The report should be accompanied by appropriate supporting evidence (e.g. URL names, printout, copies of e-mails, etc). Persons or organisations reporting incidences of misuse must provide their names and sufficient contact details (including e-mail address, telephone and fax numbers). As a rule, T-Systems will not take any action on complaints that are without supporting evidence, or are insufficiently documented.

8 User Identification and Passwords

8.1 The user identifications, passwords, access codes and addresses provided to the customer by T-Systems are intended for its personal use, and are to be protected against misuse by unauthorised persons. User identifications, passwords and access codes may not be disclosed to third parties without the prior written approval of T-Systems. If there are grounds for concern that third parties may know user identifications, passwords or access codes, they must be changed immediately, or where applicable new user identifications, passwords or access codes must be requested from T-Systems. The costs of such change will be invoiced to the customer.

8.2 The customer bears all the risks arising from the use of its user identifications, passwords and access codes, even in the case of misuse, unless T-Systems has been guilty of gross negligence.

9 Consequences of Breaches of the AUP

9.1 T-Systems reserves the right to carry out spot checks on stored and communicated content for suitability.

9.2 Where there are sound reasons to suspect a case of use in breach of applicable law or the principles of this AUP by the customer, an associated user or a third party, who has obtained services from T-Systems via the customer's system, with or without the customer's permission, T-Systems reserves the right to take such steps against such misuse as T-Systems, at its sole discretion, sees fit. These measures may include, for example, blocking access to particular services, content, systems or resources, or cutting the connection to the customer. T-Systems will give a warning prior to implementing such measures only if this is appropriate under the given circumstances, according to T-Systems' judgement.

9.3 If a material breach of this AUP by the customer is established, T-Systems may terminate its services with immediate effect and without reimbursement of fees already paid in advance.

9.4 The customer shall be liable for all damages caused to T-Systems by a culpable breach of this AUP, and it shall hold harmless T-Systems from any third party claims based on such breach.

9.5 The customer further acknowledges that in the event of a breach of this AUP, T-Systems may disclose the customer's identity to third parties.

9.6 The costs associated with the investigation of breaches of this AUP may be invoiced to the customer.