Acceptable Use Policy
supported by the Council of Hungarian Internet Providers

1. The role of Acceptable Use Policy

The present Acceptable Use Policy (AUP or Guidelines) is a set of the most important conventions adopted by the Internet Service Providers all over the world. These rules do not merely contain the recommendations concerning the attitude and behaviour described in the documents entitled „Netiquette" but they prescribe so strict demands the keeping of which shall be upheld by vindicatory sanctions.
The Acceptable Use Policy serve for the safeguard of clients using the services regularly by safeguarding the user and provider as well as its network and service against the spiteful, uneducated or perhaps neglectful users.
ISZT (Council of Hungarian Internet Providers) strongly offer to all of the Internet Providers to require of their clients to keep the Acceptable Use Policy moreover it is recommended by ISZT that the present Acceptable Use Policy is included in the General Conditions of Contract of Providers.
In case of violating the rules of Acceptable Use Policy, it is recommended for the users to inform their providers about this fact by sending their information to the following e-mail address: *abuse@<providername>.hu* proposed to maintain for this special purpose.

2. The use of Acceptable Use Policy

The fundamental principle of applying the Guidelines is that the severity of vindicatory sanction shall correspond to the severity of fault: a warning can be the first sanction, it can be followed by the cessation of services in case of a repeated infraction of the rules and finally the services shall be terminated.

3. General Guidelines

3.1. Provider has the right to terminate the service promptly without any notice in case if the Policy of Provider is violated by the activity of any of the clients. When experiencing an abusive behaviour, Provider usually prefers informing and warning the clients and warns them of stopping their illegitimate activities. However the services can promptly be suspended or terminated in case if the Policy and Rules are seriously violated and prompt damages are caused by this action.

3.2. It can never be considered a waiver of the rights from Provider's part if Provider fails or is backward in enforcing its requirements and the prescriptions of Guidelines.

3.3. It is prohibited to use the services such a way that violates any laws, rules, standards, international agreements and tariffs.

3.4. It is prohibited to violate the rules or guidelines of any networks, servers, websites, data-bases or Internet Providers (including the free services as well) that can be accessed by the client through the network of Provider.

3.5. It is prohibited to use the service for defamation and for the purpose of performing incorrect, abusive, obscene, aggressive or false activities.

3.6. The threatening, inconveniencing, insulting and terrorizing of other persons is forbidden.

3.7. It is prohibited to attack, weaken or impair the safety of any of the computers or computer-networks and to use the legitimacy of other users in an illegitimate way.
3.8. It is prohibited to gain or try to gain unauthorized access to any of the Internet endpoints or to any of the network device.
3.9. It is prohibited to disturb the operation of any of the Internet endpoints or network devices moreover the intentional overloading of network (Denial of Service) from or by using the network of Provider is not allowed.
3.10. It is prohibited to prevent other users from using the services provided by the Provider.
3.11. It is prohibited to use the network for transmitting copyrighted documents if the copyright of other persons is violated during the transmission (e.g. the transmission of pirate software is not allowed).
3.12. The intentional propagation of computer viruses and worms as well as the activity of threatening by the propagation are not allowed.
3.13. Any activities carried by any persons on the network of Provider violating the rules shall mean the violation of Guidelines and it can result in the prompt suspension or termination of service.
3.14. No one user is allowed to collect data about the other user, about the information communicated by him/her without the prior consent of the concerned user.
3.15. Clients are not allowed to observe and listen in the data proceeding through the network (sniffing).
3.16. In certain cases (e.g. when handling safety incidents or in order to eliminate the technical deficiencies), Provider is entitled to observe such a traffic but the obtained information can exclusively be used for realizing the original aim (e.g. for preventing hacking or for the elimination of deficiencies).
3.17. At the same time, Provider logs regularly certain information concerning the data traffic of users for billing and safety reasons but the obtained information recorded in the log is allowed to use exclusively for realizing the original aim.

4. Guidelines concerning the electronic mails

4.1. It is prohibited to use the network or servers of Provider for sending spam (extensive mails, high quantity of mails or unrequested commercial messages). Among others, the commercial advertisements, informative messages, caritative requests, collection of signatures and political or religious leaflets belong to this category. Messages of similar content are allowed to send only in case if this action is explicitly requested by anybody (see: Public Act on Electronic Commerce).
4.2. It is prohibited to use the network or servers of Provider for collecting replies to unrequested, high quantity or commercial electronic mails. It is prohibited to advertise any services used on the network of Provider or provided by a client in a way described in Point 4.1.
4.3. It is prohibited to forge, respectively change or remove the header of an electronic mail for deceiving purposes. However – in spite of this ban - the address of sender is altered by a lot of people sending viruses, worms or spam, therefore it is prohibited to send an automatic warning to the sender or addressee concerning the removal or disposal of viruses, worms or spam if the sender or addresser is not the own client of Provider.
4.4. It is prohibited to send a lot of copies of mails having identical or similar content. In

addition, it is not allowed to send extremely long messages or files to an addressee with the intention of disabling the user's access (mail bombing).

4.5. Without the prior consent of addressee, it is prohibited to send or forward chain letters (i.e. messages in which the addressee is requested to send the message to other users) or similar messages independent of the fact if these messages contain application for money or for other values and independent of the fact if the addressees request to receive such mails or not.

4.6. The network and servers of Provider A must not be used for receiving replies answering to mails sent from Provider B the content of which violates the Guidelines prescribed by the Provider A or B.

4.7. In case if a user uses the service of an other Internet Provider for advertising a webpage placed at that certain Provider, he/she is obliged to use the advertisement methods corresponding to the prescriptions of Guidelines.

5. Guidelines relating to contacts

The client shall denominate one or more contact persons („contact person") who are responsible for all the computers, computer-networks or sub-networks linked to the Internet by the service offered by Provider. Before configuring the network connection, client shall give the contact persons' names, telephone-numbers, postal- and e-mail addresses („contact" information). The „contact" information shall be up-to-date and exact at any time therefore the service representative of Provider shall promptly be informed about the incidental changes. The contracting party bears the responsibility of damages arising owing to the improper and outdated information.
The contact person shall have the suitable devices, access-possibility and authority to configure and operate the systems of contracting party and/or to restrict the access to them.

6. Guidelines relating to the shared resources

The Internet service of a Provider is based on shared resources. The excessive use or abuse of these resources (i.e. the use of these resources beyond measure) by even one subscriber can have a negative effect on all of the other users. The abuses of network resources can decrease the throughput of network and are contrary to the Guidelines. These abuses can result in the suspension or termination of service.

7. Installation of an Open Recursive Name Server

The clients must ensure that in case they wish to operate a name server on their own, the technical personnel operating it is familiar with the global DNS. Moreover, they will operate it in such a manner that they will not endanger, not even by negligence, the functioning of the DNS. Such a threat is the operation of an open (i.e. available to anyone) recursive name server, that allows a possible attacker to make the services of a third party unavailable (DoS, i.e. Denial of Service attack). This threat is even more serious if the client's name server is DNSSEC capable. Therefore the client must ensure that they operate an Open Resolver only if they can guarantee that they are able to apply measures to filter out such attacks and they provide a point of contact for such cases, and treat these requests as a matter of urgency. Besides, the clients must inform in advance their access provider of such an intention to operate an Open Recursive Name Server and they must co-operate with them closely during the operation.

8. Amendment of the Acceptable Use Policy

Provider is entitled to actualize the Guidelines or change the conditions of contract in accordance with the actualized Guidelines but Provider is obliged to publish the authoritative text on the page indicated in advance (preferably it can be the „General Conditions of Contract" as well as a webpage).

V1.1. Last modified:09.04.2013