BIX Charter

Rules of operation and use of the BIX

Last modified: by the ISzT General Meeting on 23 April 2015

Enters into force on 1 May 2015

1. Major purpose of the BIX (**B**udapest **I**nternet E**x**change) is to prevent the Hungarian and regional internet traffic between the different internet service providers from loading *international* connections of the internet service providers and to provide a platform for exchanging IP based traffic between different internet service providers.

2. Terms

   a) *BIX:* is a network system distributed geographically, which consists of *BIX service access points* and data transmission connections connecting them. Users of the BIX - the *BIX members* - can connect their own networks at the BIX service access points.

   b) *BIX member:* an internet service provider connected to the BIX with its own network via a BIX service access point (using the proper device or data transmission connection). A BIX member can only be an internet service provider that fulfils the requirements defined in Section 3. and accepts and adheres to the rules of the operation and use of the BIX defined hereunder. Regarding the connection to the BIX, BIX members may freely select their BIX service access points.

   c) *BIX service provider:* BIX is operated by ISzT (name: Internet Szolgáltatók Tanácsa - Council of Hungarian Internet Service Providers, address: 1132 Budapest, Victor Hugo u. 18-22.) .

   d) *BIX Committee*: body within the framework of ISzT (Internet Szolgáltatók Tanácsa - Council of Hungarian Internet Service Providers). The Committee sets the rules of using the BIX and supervises its operation. Members of the BIX Committee are those ISzT members who are also BIX members at the same time. Each member of the BIX Committee has one vote. The chairman of the BIX Committee is elected by the General Assembly of ISzT every year. It is the duty of the chairman to coordinate the activities of the BIX Committee, to convene Committee meetings and to administer membership application procedures. All BIX members are entitled to join the open meetings of the BIX Committee.

   e) *BIX service*: Service provided by the BIX service provider to the BIX members connecting the network of the BIX members to the BIX internet exchange. Conditions of the BIX service not regulated in this document are subject to the separate BIX service agreement between the BIX service provider and the BIX member.

3. Eligibility requirements concerning BIX membership

a) Any service provider is entitled to BIX membership, if they hold their own AS Number and IP prefixes which are registered in the RIPE Database (aut-num, inetnum, inet6num, route, route6).

   Service providers conforming to these requirements are eligible for a simplified membership application procedure. The requirements must be met continuously. Eligibility is checked at half year intervals and membership can be cancelled in case of not conforming to the requirements.

b) Furthermore, a provider is eligible for BIX membership if the application - justified by special reasons - is approved by the BIX Committee during the General Assembly of ISzT by majority vote. The decision of the special judgment details the duration and the conditions of the special membership.

c) In case of special obligation by law an "authority specific" service can be provided to the authorized organization. The terms of this service can be different from those of the general BIX services.

4. Peering categories

   Every BIX member is free to decide how to exchange traffic with other BIX members within the following categories:

   a) Open/Free peering: Unlimited and free peering with other BIX members. Members of the "Free peering" category are obliged to:

      I. use the BIX Route servers,

      II. peer free of charge with any BIX member (irrespectively of the peering category of the other member) regarding the traffic within Hungary and in case of request of the other BIX member except:

         i. its own IP-Transit customer, or

         ii. with members whom it has private peering connection with.

   b) Selective peering: peering with other BIX members based on request of the other BIX member using a case by case decision.

   c) Restrictive peering: peering with other BIX members only by own initiative.

5. BIX fees

   a) BIX fees are defined by the BIX Committee.

   b) BIX fees are published in the Appendix "BIX Fees".

c) In line with the basic BIX policy the BIX Committee encourages the free and unlimited peering of the domestic traffic. For this reason members assuming open/free peering are entitled to discount.

d) Discounted fee applies to standby ports.

6. Technical requirements concerning BIX connections

a) BIX members can be connected to one or more ports of a BIX Ethernet switch with a router or a data transmission device establishing a direct layer 2 (data connection level) connection. On one port of the BIX switch only one MAC address is allowed.

b) BIX members must not use the BIX to transmit their internal traffic. A member can be connected to BIX via more than one port and/or at more than one BIX service access point, but multipoint connection may only serve load balancing or backup purposes.

c) BIX itself is a geographically distributed system. The distributed system consists of BIX service access points, connected to each other with direct layer 2 (data connection level) connections with backup. BIX members can connect to BIX using the interfaces of BIX Ethernet switch(es) located at BIX service access points. The optical transceiver (corresponding to the selected connection type) at the BIX switch is part of the BIX service and it is included in the BIX fee. The BIX member is obliged - at its own expense - to ensure that its connecting interface is compatible with the selected connection type. Members have to use optical cable connection to the BIX service access points, copper cable connections are not allowed.

d) Only BGP4 external routing protocol can be used on BIX. The possession of a valid, registered AS number by the service provider and the internet accessibility of networks that are going to be advertised are prerequisites of BIX membership.

e) IP addresses used on BIX shall be allocated from an independent address block dedicated to this purpose. Addresses are allocated by the BIX service provider.

f) There are route servers in operation on BIX, based on the information located in the RIPE objects (route, aut-num).

g) The BIX member is obliged to maintain the RIPE object entries according to the actual situation.

h) The BIX member is entitled to advertise on BIX only networks that fall

- within its own address range,
- within the address range of its customers,
- within the address range of its backup partners.

The advertisements must be aligned with the RIPE entries.

i) The BIX member may forward to BIX only IP packages with source addresses that can also be advertised by that member. In order to ensure this, the BIX member is obliged to apply properly set filters in its routers.

7. Traffic of the Ethernet switches operated at the BIX service access points is measured and supervised by the BIX service provider, the traffic information is made available to the public on the BIX website.

8. BIX service provider commits to provide any kind of assistance and contribution - within reasonable frames of the technical possibilities - to the BIX member in order to implement the access to the equipment installed on BIX using the telecommunication solution owned by or available to the BIX member, including access to the building (cable, antenna) and the establishment of the admission within the building (the related expenses must be compensated by the member).

9. The right for BIX membership (or losing such rights) is investigated and determined by the BIX Committee. It is also investigated and identified by the BIX Committee, which conditions are met by the members and whether they adhere to the rules. An appeal against the resolution of the BIX Committee is to be submitted to the IszT General Assembly, which investigates righteousness of the resolution.

10. Applications for the BIX membership can be submitted in writing to the BIX Committee (posted or electronically, using the bix@iszt.hu e-mail address). All certifications and information making possible the resolution of the Committee regarding the rights of the applicant must be enclosed. The application - if conditions of the simplified procedure are met - is approved by the BIX Committee on-line: the application is forwarded to the BIX members for comments or questions within a week. If there are no questions or the answers are satisfactory, the Chairman of the BIX Committee notifies the applicant and the prospective member can proceed by signing the BIX service contract with the BIX service provider. Applications not eligible for the simplified procedure will be discussed at the next General Assembly of ISzT.

11. In case if - after multiple notices - the BIX member does not adhere to the rules set forth, then the BIX Committee conducts an investigation and after considering all circumstances (does the breach of the rules occur by the negligence of the BIX member or it is due to external reasons; is the breach a first instance or it occurs repeatedly, etc.) the BIX service provider may bind the BIX member to pay an extra charge (between HUF 100,000.00 and 500,000.00 not including VAT). In very serious case the right for the BIX membership must be called off.

12. Access of BIX members causing continued operational disturbances or failures of the BIX operation can be restricted by the BIX service provider without prior notice. The BIX service provider must notify the restricted BIX members about the fact of and reasons for the restriction within 24 hours.

13. BIX members are obliged to:

    a) publish a public e-mail address on the BIX web site to receive error messages from the BIX members and BIX service provider. BIX member is obliged to reply the error messages sent to its e-mail address within 24 hours,

b) provide an emergency telephone number to the BIX service provider, available 24 hours a day.

14. Peering connections established on BIX are regarded by BIX members as effective peering connections based on mutual agreement.

15. The following Appendices are an integral part of the present Charter:

Appendix 1. - Acceptable Use Policy (AUP) supported by the Council of Hungarian Internet Providers"

Appendix 2. - BIX Fees

Appendix 1. - 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. It is prohibited to gain or try to gain unauthorized access to any of the Internet endpoints or to any of the network device.
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.

3.8. It is prohibited to prevent other users from using the services provided by the Provider.

3.9. 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).

3.10. The intentional propagation of computer viruses and worms as well as the activity of threatening by the propagation are not allowed.

3.11. 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.

3.12. 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.

3.13. Clients are not allowed to observe and listen in the data proceeding through the network (sniffing).
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).
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

Appendix 2. - BIX Fees

as of 11th of May 2016

a) BIX fees in HUF

Port/ service	Active port monthly fee with Open/Free peering(1)	Active port monthly fee with Selective/Restrictive peering(1)	Set-up (one time) fee (net HUF)
1 Gbps (first port)	HUF 30 000	HUF 48 000	HUF 30 000
1 Gbps (further ports)	HUF 60 000	HUF 96 000	HUF 60 000
10 Gbps (first 3 ports)	HUF 150 000	HUF 240 000	HUF 0(2)
10 Gbps (further ports)(3)	HUF 100 000	HUF 160 000	HUF 0(2)
40 Gbps	HUF 500 000	HUF 800 000	HUF 500 000
50 Gbps(4) (on 100 Gbps port)	HUF 500 000	HUF 800 000	to be discussed
80 Gbps or 90 Gbps or 100 Gbps(3) (on 10 Gbps ports)	HUF 900 000 Ft	HUF 1 440 000 Ft	HUF 0(2)
100 Gbps(5)	HUF 900 000	HUF 1 440 000	HUF 0(5)
Private VLAN	HUF 10 000/ VLAN / year		HUF 10 000

b) BIX fees in EUR

Port/ service	Active port monthly fee with Open/Free peering[1]	Active port monthly fee with Selective/Restrictive peering[1]	Set-up (one time) fee (net HUF)
1 Gbps (first port)	EUR 99	EUR 158	EUR 99
1 Gbps (further ports)	EUR 198	EUR 317	EUR 198
10 Gbps (first 3 ports)	EUR 495	EUR 792	EUR 0[2]
10 Gbps (further ports)[3]	EUR 330	EUR 528	EUR 0[2]
40 Gbps	EUR 1 650	EUR 2 640	EUR 1 650
50 Gbps[4] (on 100 Gbps port)	EUR 1 650	EUR 2 640	to be discussed
80 Gbps or 90 Gbps or 100 Gbps[3] (on 10 Gbps ports)	EUR 2 970	EUR 4 752	EUR 0[2]
100 Gbps[5]	EUR 2 970	EUR 4 752	EUR 0[5]
Private VLAN	EUR 40/ VLAN / year		EUR 40

Notes:

(1) Open/Free, Selective/Restrictive peering: see BIX Charter, paragraph no. 4.

- Prices do not include the VAT!

Discounted prices for standby (reserve) ports:

- The fee for a standby port provided on the same BIX node is 40% of the active port fee.
- The fee for a standby port provided on different BIX node is 40% of the active port fee.

Promotions:

- The fee of the first 1 Gbps port for Free peering is HUF 30k (EUR 99)

(2) Promotion till 15th December 2016: the set-up of the 10 Gbps ports is free.

(3) 10 Gbps port volume discount: the monthly fee beginning with the 4th port is HUF 100k (EUR 330) for Free Peering; beginning from the 8th port (80 Gbps, 90 Gbps, or 100 Gbps) the total monthly fee is equal to the 100 Gbps port fee.

(4) Promotion till 31st December 2016: 50 Gbps on a 100 Gbps port costs HUF 500k (EUR 1,650) for Free peering. If the traffic exceeds 50Gbps for the 5% of the time period the total 100 Gbps port fee shall be paid.

(5) Promotion till 15th December 2016: for the first 3 customers signing up for 100 Gbps on a 100 Gbase-SR10 port the set-up fee will be waived. Applies for the first active port of the customer.