THE FENIX PROJECT CONNECTION RULES

1. PRELIMINARY PROVISIONS

1.1. These Rules set out the conditions for connecting to the FENIX project (hereinafter "**FENIX**") set up by the above-cited Founders as part of the NIX.CZ Association.

1.2. FENIX is set up in compliance with the applicable Operating Rules, Service Rates and Articles of Association of NIX.CZ Association (hereinafter "**NIX.CZ**").

1.3. These Rules also fully apply to the Founders, including the possibility of being expelled from FENIX.

1.4. FENIX serves as a means of emergency communication for the members/customers of NIX.CZ, providing a high level of confidence and security in the event of a major attack on the internet infrastructure.

1.5. FENIX was created with the aim of providing a "last resort" connection in case a FENIX member's infrastructure should become the target of an attack.

1.6. Joining FENIX is free of charge

1.7. NIX.CZ is not the Founder but a part of FENIX, it may be connected to it at any time and enjoys the same rights to its use as the rest of FENIX members

2. CONDITIONS FOR NEW MEMBERS OR CUSTOMERS OF NIX.CZ JOINING FENIX

2.1. In order to become a member of FENIX, a member/customer must have been connected to any NIX.CZ node for a period longer than six months.

2.2. A candidate for FENIX membership must declare in writing that in the case of being admitted to FENIX membership they shall adhere to the present Rules. In addition, they must provide: references from at least two existing FENIX members that they should be accepted to join FENIX; a statutory declaration regarding their compliance with the conditions listed in Article 2; and a copy of the standard Agreement or Terms of Conditions used with their customers.

2.3. Any existing member of FENIX can comment on a membership application. If within fourteen days after the existing members of FENIX have been informed about a membership application no group of minimum six existing members has protested the application, the candidate can be connected to FENIX and become a member. Admission to FENIX membership is not a legal right, not even in case that all the conditions listed in Clause 2.5. have been met.

2.4. Membership is closed to those NIX.CZ customers who are connected to a NIX.CZ node as part of a partnership scheme, where the partner is another member/customer of NIX.CZ.

2.5. A member/customer of NIX.CZ may submit a valid membership application provided that:

2.5.1. A FENIX applicant must actively participate in the workgroups and in case of membership also in the voting procedures of the statutory bodies of NIX.CZ at least once a year;

2.5.2. they have no overdue liabilities towards NIX.CZ and within the previous six months has not had any outstanding liabilities due for more than 15 days;

2.5.3. they have not repeatedly or seriously violated the NIX.CZ Operating Rules or Articles of Association;

2.5.4. they operate fully redundant, non-overloaded and independent connections to at least two of NIX.CZ nodes, so that should all connections passing through one node fail, the other node(s) can take over automatically and carry normal data traffic exchanged with partners within NIX.CZ without the risk of congestion; i.e. exceeding the 95th percentile of aggregate traffic on the rest of available links[1].

2.5.5. they contractually ban their customers from carrying out any illegal activities on the network (spamming, attacks, etc.);

2.5.6. they use both IPv4 and IPv6 protocols on their network, while actively using both protocols to connect to the NIX.CZ nodes, to provide access to web presentations and allocate them to customers;

2.5.7. their domains, which it uses to communicate with customers/business partners (including company websites and product websites), are signed by DNSSEC technology, using the latest available algorithms and security standards, unless such signing is prevented by serious technical issues, and the validation on their resolvers has been turned on;

2.5.8. their Network Operations Center (NOC) functions smoothly 24-hours a day, 7 days a week, with an email contact and at least one telephone number which is available even in case of a massive DDoS attack targeted at the infrastructure of the member listed on the NIX.CZ intranet. The phone number must be a direct line to a technician able to deal with the problem and must not rely on IVR technology;

2.5.9. they use source address filtering on their network or its parts, which is announced into the FENIX VLAN (to prevent IP spoofing), in the sense of either BCP-38 or SAC004. For IP addresses in the member's own AS the granularity must be at least /24 for IPv4 and /48 for IPv6. Prefixes learned from the FENIX VLAN must be re-advertised to only those ASNs, whose prefixes are advertised within the FENIX project.

2.5.10. they have a system for detecting and eliminating sources of attacks similar to and including DNS amplification (banning unmanaged open resolvers, implementing response rate limiting);

2.5.11. they monitor both backbone traffic and customer connections at least in terms of data flows and transmitted packages (such as MRTG or similar); this monitoring must be able to actively detect and signal an irregularity in the monitored values;

2.5.12. they do not use the BGP protocol to advertise other prefixes than those they are allowed to advertise;

2.5.13. they do not send traffic into the FENIX VLAN from prefixes their network is not authorised to advertise;

2.5.14. they protect their routers in compliance with the RFC6192 (control plane policy) recommendations or in another similarly effective way;

2.5.15. they operate a CERT/CSIRT team which is at least "listed" with the Trusted Introducer service (http://www.trusted-introducer.org);

2.4.16. they have implemented internal incident resolution procedures;

[1] In a floating time interval of 720 hours the other connections must be able to absorb all data traffic exchanged with NIX.CZ partners with a tolerance / exception of any 432 five-minute intervals (representing 5 percent of 720 hours) within this period the highest volume (ie 432
operationally significant five-minute intervals that are ignored in evaluation).

2.5.17. they intervene to remove/limit a security incident as quickly as possible, within, at the latest, 30 minutes after it has been declared;

2.5.18. they monitor security messages from the suppliers of network components and react to them as appropriate;

2.5.19. all of their websites where they communicate with their customers or business partners, are permanently redirected to HTTPS with TLS certificate trusted in the most popular web browsers, without mixed content, and no ciphers which are considered unsafe.

3. OPERATIONAL PREREQUISITES FOR JOINING FENIX

3.1. FENIX members:

3.1.1. actively participate in workgroups and FENIX voting procedures;

3.1.2. monitor the communication on the special FENIX members' mailing lists;

3.1.3. are part of a RTBH (Remotely-Triggered Black Hole Filtering) filtering system, which mitigates the impact of DDoS attacks. RTBH allows the network that has become the target of an attack to identify, using an appointed BGP community's designation, which part of the traffic will be blocked on the side of NIX.CZ;

3.1.4. use a FENIX-operated Route Server, especially in order to connect to the RTBH filtering system described in Clause 3.1.3. and to connect with other FENIX members.

3.2. Does not use their FENIX connection as the main platform for connecting to the NIX.CZ node, unless required by a technical issue, which the FENIX member has announced via the mailing list.

3.3. The FENIX connection uses a physical port or a 802.1Q.

3.4. Within the FENIX, BGP sessions are protected against session hijacking.

3.5. A FENIX member must guarantee the appropriate application of the rules of Article 2.5 and Article 3 to at least the part of the network whose ranges they promote within the FENIX VLAN.

4. MONITORING RULE COMPLIANCE

4.1. Adherence to these Rules is monitored by the NIX.CZ staff, who are authorized to carry out regular tests to ensure compliance (and to this aim are authorized to violate these Rules). Identified violations will be announced to FENIX members. The member concerned is allowed to comment on the findings; other members can demand clarification or additional information.

4.2. Upon the violation of these Rules, including cases where a FENIX member no longer complies with the conditions outlined in Clause 3, the Director of NIX.CZ can decide to expel the member from FENIX. Reentering FENIX is then only possible through the procedure outlined in Clause 2.

5. RULE CHANGES AND OTHER DECISIONS; COMMUNICATION

5.1. Any member of FENIX can suggest a change to the present Rules. Once the proposal has been discussed, the Director of NIX.CZ asks the members of FENIX to vote. In order to be accepted, the proposal must receive an absolute majority of all of the FENIX members' votes.

5.2. All communication between FENIX members happens via the special mailing list.

5.3. Each FENIX member has the obligation to provide other members with information about significant security incidents that FENIX is supposed to prevent.

5.4. FENIX members vote using an electronic voting system implemented by NIX.CZ.

5.5. Each FENIX member is obliged to maintain confidentiality regarding the facts they have learned as members of FENIX, including and especially: all information exchanged through member communication; information about security incidents detected on other members' networks; information regarding the compliance or violation of the prerequisites set out by these Rules; information about rejected applications for membership in FENIX. This information can only be made public if the member concerned has explicitly agreed to its publication and, in cases where the source of the information is unknown, when all members of FENIX have agreed that this information be made public.

5.6. In the case of a dispute about the interpretation of any of these Rules, especially when deciding whether or not one of the provisions in these Rules has been violated, the final decision rests with the Director of NIX.CZ.

6. PUBLICITY

6.1. Each FENIX member has the right to use the special FENIX logo in the form approved by FENIX members.

6.2. On its website, NIX.CZ publishes a special list of FENIX members, explaining the significance of FENIX.