AIXP Memorandum of Understanding

The undersigned, representative of _____ (ISP), hereby confirms the participation of the above mentioned ISP in the Arusha Internet Exchange (AIXP). The Technical and Organizational Requirements below are accepted and will be adhered to.

Company Name: _____
Address: _____
_____
_____
Admin Contact: _____ (Name)
_____(Email)
Technical Contact: _____ (Name)
_____(Email)
Signature: _____
Name in print: _____
Date: _____
Filled by AIXP:
Port on AIXP switch: _____
IP on AIXP net: 196.223. __ . ___
ASN: _____

A. Technical requirements

1. Peers will be provided with 2U rack space. There might be restrictions in the future when capacity is limited.
2. AIXP provides its participants with a layer-2 Ethernet switch fabric and a layer-3 route server.
3. Participants may only connect equipment which they own and operate themselves to the AIXP. They may not connect equipment on behalf of third parties.
4. Peers may only utilize a single layer- 2 MAC address to directly connect a single layer-3 router per port allocated from the AIXP switch fabric.
5. It is preferred that each participant have their own Autonomous System number, peers without an ASN allocation will be assigned an ASN from private ASN space by the AIXP Management Committee. Any peer who has previously been connected to the AIXP using private ASN and then later acquires their own public ASN must notify the AIXP Management Committee as soon as possible in order to incorporate this development into the BGP peering at AIXP.
6. AIXP participants will advertise routes to their IP address range(s) to the AIXP route server(s). Peers shall not advertise routes other than their own, without the prior written permission of the assigned holder of the address space.
7. Peers shall not advertise a next-hop other than their own.
8. Peering between routers across AIXP will be via BGP
9. Peers shall not generate unnecessary route flap, or advertise unnecessarily specific routes in peering sessions with other participants across AIXP.
10. Peers shall not point their default route to the AIXP.
11. Participants must, on all interfaces connected to the AIXP switch fabric, disable Proxy ARP, ICMP redirect, CDP, IRDP, directed broadcasts, IEEE802 Spanning Tree, any interior routing protocol broadcasts, and any MAC layer broadcasts other than ARP or inverse-ARP.
12. Peers must set netmasks on all interfaces connected to the AIXP to include the entire AIXP peering LAN.
13. Participants shall not announce ("leak") prefixes including some or all of the AIXP peering LAN to other networks without explicit permission of AIXP.
14. Participants must clearly label all equipment that resides at the AIXP facility with ownership and contact information.
15. Participants will not touch equipment and/or cabling owned by other participants and installed at AIXP or in the room containing the AIXP without the explicit permission of the participant who owns the equipment.
16. Peers should not routinely use the AIXP switch fabric for carrying traffic between their own routers.
17. Participants will not install traffic monitoring software to monitor traffic passing through AIXP, except through their own ports. AIXP may monitor any port
18. AIXP does make statistics of the aggregate traffic flow over the exchange switch available to the public.
19. Participants shall endeavor to provide advance notice via email to each of their BGP peers, in the event that a service disruption or discontinuity of BGP peering can be foreseen.

For clarification:

1. ISPs should advertise all their networks to the IXP.
2. ISPs should not use multiple links to the IXP for the purpose of routing their internal traffic.
3. ISPs should accept all routes advertised by all other peers and route traffic through the Exchange (the purpose of it).

B. Organizational Requirements

1. Participants have a duty of confidentiality to the other AIXP Participants in AIXP affairs.
2. Peers must provide 24x7 contact details for use by AIXP staff.
3. In matters of AIXP, the primary means of communication will be via email.
4. Peers must not refer customers or customers' agents to AIXP staff. All queries must be directed through the peer's support staff.
5. Peers must not carry out any illegal activities through AIXP. They are to obey the laws of the country.
6. Participants will pay annual fees in advance. Failure to do so will result in immediate

disconnection. Fees are detailed in Annex C below. It is Participants' responsibility to ensure that all contact information held by AIXP in connection with their participation is correct and up to date.

7. All applications to join the AIXP must follow the correct joining procedure as follows: Applications will be accepted, provided this MoU including the Technical and Organisational Requirements as well as the Fees are accepted and the MoU is signed and necessary details given. Applications must be accompanied by the setup fee and the full port connection fee for the current calender year.
8. Any complaints must be referred in writing to the AIXP Management Committee of TISPA. The working group will discuss them at the next meeting. The decision can be revised by the Board of TISPA, in which case that will be final.
9. The AIXP will not provide rebates of any sort for down time. TISPA and AIXP do not warrant or assume any liability or responsibility for services provided or not provided.
10. Participants of the AIXP must give 3 months notice in writing to TISPA if they intend to stop using the IXP. There will be no refund on charges under any circumstances.

C. Fees schedule

AIXP will charge each participant a port connection fee. This will allow the peer to connect to the designated 10/100Mbit port on the AIXP switching fabric.
The fee is set to USD 500.00 for one calendar year, payable in advance. A once-off registration fee of USD 1,000.00 will be charged.