ZIXP Memorandum of Understanding

The undersigned, representative of ___________________ (participant), hereby confirms the participation of the above mentioned organisation in the Zanzibar Internet Exchange (ZIXP). The Technical and Organizational Requirements below are accepted and will be adhered to.

Company Name: ___________________________

Address: ___________________________
____
____

Admin Contact: _______________________ (Name)
_______________________ (Email)

Technical Contact: _______________________ (Name)
_______________________ (Email)

ASN: ____________

Signature: ___________________________

Name in print: ___________________________

Date: ___________________________

Filled by TISPA:

Port on ZIXP switch: _______ switch: ______

IP on ZIXP net: ____________

A. Technical requirements

1. ZIXP provides its participants with a layer-2 Ethernet switch
2. fabric connecting several peers, and BGP route servers.
3. Participants may only connect equipment which they own and operate themselves to the ZIXP. They may not connect equipment on behalf of third parties.
4. Peers may only utilize a single layer-2 MAC address to place a single layer-3 router per port allocated from the ZIXP 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 ZIXP Management Committee. Any peer who has previously been connected to the ZIXP using private ASN and then later acquires their own public ASN must notify the ZIXP Management Committee as soon as possible in order to incorporate this development into the BGP peering at ZIXP.
6. ZIXP participants are encouraged to advertise all routes to their own and their customers' IP address range(s) to the ZIXP route servers. Peers shall not advertise routes other than the above, 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 ZIXP will be via BGP-4.
9. Peers shall not generate unnecessary route flap, or advertise unnecessarily specific routes in peering sessions with other participants across ZIXP.
10. Peers shall not point their default route to the ZIXP or any peer.
11. Participants must, on all interfaces connected to the ZIXP 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, on all interfaces connected to the ZIXP switch fabric, disable any duplex, speed, or other link parameter auto-sensing.
13. Peers must set netmasks on all interfaces connected to the ZIXP to include the entire ZIXP peering LAN.
14. Peers shall avoid congestion on their interfaces or transmission links at or into ZIXP so as to not cause unwanted latency for traffic at ZIXP.
15. Participants shall not announce ("leak") prefixes including some or all of the ZIXP peering LAN to other networks without explicit permission of ZIXP.
16. Participants must clearly label all equipment that resides at the ZIXP facility with ownership and contact information.
17. Participants will not touch equipment and/or cabling owned by other participants and installed at ZIXP or in the room containing the ZIXP without the explicit permission of the participant who owns the equipment.
18. Peers should not routinely use the ZIXP switch fabric for carrying traffic between their own routers.
19. Participants will not install traffic monitoring software to monitor traffic passing through ZIXP, except through their own ports. ZIXP may monitor any port but will keep any information gathered confidential, except where required by law or where a violation of this Memorandum of Understanding has been determined by TISPA.
20. 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. ZIXP does make statistics of the aggregate traffic flow over the exchange switch available to the public.

B. Organizational Requirements

1. Participants have a duty of confidentiality to the other ZIXP Participants in ZIXP affairs.
2. Peers must provide 24x7 contact details for use by ZIXP staff.
3. In matters of ZIXP, the primary means of communication will be via email.
4. Peers must not refer customers or customers' agents to ZIXP staff. All queries must be directed through the peer's support staff.
5. Peers must not carry out any illegal activities through ZIXP. 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.
7. It is participants' responsibility to ensure that all contact information held by ZIXP in connection with their participation is correct and up to date.
8. All applications to join the ZIXP must follow the correct joining procedure as follows:
9. 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 port connection fee for the current calender year.
10. Any complaints must be referred in writing to the ZIXP 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.
11. The ZIXP will not provide rebates of any sort for down time. TISPA and ZIXP do not warrant or assume any liability or responsibility for services provided or not provided.
12. Participants of the ZIXP 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

Fees as published by TISPA and amended from time to time do apply.