GIX Technical Requirements APPENDIX A

Members are expected to adhere to the Technical Requirements of GIX.

1. Members may only connect equipment that is owned and operated by that Member to GIX. Members may not connect equipment to GIX on behalf of third parties.

2. Members must only use IP addresses on the interface(s) of their router(s) connected to the GIX allocated to them by the GIX.

3. Members may only present a single MAC address to any individual GIX port that is allocated to them.

4. Peering between Members' routers across GIX will be via BGP-4.

5. Members shall not generate unnecessary route flap, or advertise unnecessarily specific routes in peering sessions with other Members across GIX.

6. Members may not advertise routes with a next-hop other than that of their own routers without the prior written permission of the advertised party, the advertisee, and GIX.

7. Members may not forward traffic across GIX unless either the traffic follows a route advertised in a peering session at GIX or where prior written permission of the Member to whom the traffic is forwarded has been given.

8. Members must, on all interfaces connected to the GIX, disable: Proxy ARP, ICMP redirects, CDP, IRDP, Directed broadcasts, IEEE802 Spanning Tree, Interior routing protocol broadcasts, and all other MAC layer broadcasts except ARP.

9. Members must, on all interfaces connected to GIX, disable any duplex, speed, or other link parameter auto-sensing.

10. Members shall not announce ("leak") prefixes including some or all of the GIX peering LAN to other networks without explicit permission of GIX.

11. Members must set net masks on all interfaces connected to GIX to include the entire GIX peering LAN.

12. Any equipment and/or cabling installed by a Member at GIX must be clearly labeled as belonging to the Member.

13. Members will not touch equipment and/or cabling owned by other Members and installed at GIX or in the room containing the GIX without the explicit permission of the Member who owns the equipment.

14. Members will not install 'sniffers' to monitor traffic passing through GIX, except through their own ports. GIX 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 GIXA Board.

15. Members will not circulate correspondence on confidential GIX mailing lists to non-members.

16. Members must ensure that their usage of GIX is not detrimental to the usage of the GIX by other Members.

17. Members may not connect more than two wide-area circuits to routers housed at GIX. This restriction may be overridden on a per-case basis at the discretion of GIXA Board.

18. Members may not directly connect customers who are not GIX members via circuits to their router housed in any GIX rack.

19. Members should not routinely use the GIX for carrying traffic between their own routers.

20. The technical committee will set up certain monitoring features on the server at the GIX. Certain GIX members will be asked to have their ops departments monitor these features such that any problems can be referred to GIX technical support personnel as quickly as possible.

21. Each ISP is required to assign the following to the GIX to peer successfully
    Technical Person responsible for administrating and setting up of the GIX
    A BGP-4 Enabled Router
    A public AS Number
    A RO SNMP Community for monitoring of traffic usage

Traffic usage; all service providers need to make available their RO SNMP community of their routers for monitoring of traffic. This will be published to web portal for all members of the GIX to view and monitor