TERMS & POLICIES FOR RINEX

INTRODUCTION

On February 2014, The Rwanda Utilities and Regulatory Authority – "RURA", and the Rwanda Internet Community and Technology Alliance "RICTA" former "Rwanda information and Communication Technology Association" – "RICTA Ltd.", hereinafter referred to as "RINEX Management", have entered a Memorandum of Understanding that gives RICTA the mandate and authority to manage, operate and develop the Rwanda Internet Exchange (Point), herein called "RINEX". This document sets the policies that will guide the management and operations of RINEX.

DEFINITIONS OF TERMS

In this policy document, unless the context otherwise requires:

1. **"RINEX Management"** refers to RICTA management.
2. **"The Internet"** is a network of networks, interconnected in Peering and Transit relationships collectively referred to as a Global Internet Peering Ecosystem. [Source: DrPeering.net].
3. **"Internet Protocol – IP"** a communications protocol for computers connected to a network, especially the Internet, specifying the format for addresses and units of transmitted data. It is the method or protocol by which data is sent from one computer to another on the Internet.
4. **"Autonomous System – AS"** is a group of IP networks run by one or more network operators with a single clearly defined routing policy. Alternatively, an AS can be defined as a set of routers under the same administrative control.
5. **"Autonomous System Number – ASN"** An ASN is a globally unique number used to identify an Autonomous System. It enables an AS to exchange exterior routing information with neighboring ASes.
6. **"Border Gateway Protocol – BGP"** is an inter-Autonomous System routing protocol, also known as Exterior Gateway Protocol (EGP). It enables to create an IP network free of routing loops among different autonomous systems.
7. **"Layer-2"** refers to the Data Link layer of the commonly referenced multi-layered communication model, Open Systems Interconnection (OSI). The Data Link layer is concerned with moving data across the physical links in the network. In a network, the switch is a device that redirects data messages at the layer-2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.
8. **"Internet Service Providers (ISPs)"** connect end-users and businesses to the public Internet. [Source: DrPeering.net]
9. **"A Content Distribution Network (CDN)"** is a company that operates a network that distributes

and disseminates content to the edge of the access networks across Internet Regions. CDNs distribute the content to the edge, as close to the eyeballs as practicable. [Source: DrPeering.net]

10. **"Internet Peering"** is the business relationship whereby companies (Internet Service Providers (ISPs), Content Distribution Networks (CDNs), Large Scale Network Savvy Content Providers) reciprocally provide access to each other's customers. [Source: DrPeering.net]
11. **"Internet Transit"** is the business relationship whereby one ISP provides (usually sells) access to all destinations in its routing table. [Source: DrPeering.net]
12. **"A peer" or "A RINEX participant"** is any organization or entity that participate in an Internet Exchange Point
13. **"Paid Peering" is** the business relationship whereby companies (Internet Service Providers (ISPs), Content Distribution Networks (CDNs), Large Scale Network Savvy Content Providers) reciprocally provide access to each other's customers, but with some form of compensation or settlement fee. Source: DrPeering.net]
14. **"Public Peering"** is Internet Peering across a shared (more than two party) peering switch fabric [Source: DrPeering.net]
15. **"Private Peering"** is Internet Peering across transport with exactly two parties connected to it, usually a fibre cross connect or point to point circuit. [Source: DrPeering.net]
16. **"Application Form"** means the application form, which is referenced in clause 15.
17. **"Connection"** means the physical connection of your router (directly or via a third party network) to the RINEX infrastructure.
18. **"Fee"** means the fee payable to RICTA Ltd. for the connection to RINEX. The RINEX Fees are defined in Section 8 of this document.
19. **"RINEX"** The Rwanda Internet Exchange (Point).
20. **"RINEX member"** or **"The operator"** or **"The participant"** or **"The peer"** means any organization officially admitted to connect to RINEX.
21. **"RINEX Peering LAN"** means a layer-2 Ethernet network allowing the exchange of traffic between RINEX peering members.
22. **"Peer interface"** means the physical or logical port (VLAN), which connects a peer to the RINEX network.
23. **"Regional Internet Registries"** means the bodies appointed by the Internet Assigned Numbers Authority to be responsible for the allocation of Internet Number Resources in a specific geographic region to their members.
24. **"Point of Presence"** or **"POP"** is primarily the infrastructure that allows remote users connect to the Internet or to an operator's network.

OPERATIONAL REQUIREMENTS

25. All applications to join RINEX must follow the correct/approved joining procedure, as set in "Procedure for Joining RINEX".
26. It is the operator's responsibility to ensure that all contact details information held by RINEX management in connection with their participation in RINEX is correct and up to date.
27. RINEX is built on 10/100/1000Base-T Ethernet technology. It is a Layer-2 service with no routing features within the Exchange point switch. The Operator's router is responsible for the routing of

the packets through the exchange point. RINEX operates route server(s) that aim at facilitating new entrants to connect to the rest of RINEX participants without initiating a single BGP session with each existing customer.

28. All installed infrastructure equipment has redundancy from electrical breakdown for high reliability demands.
29. RINEX switch consists of one VLAN, VLANN #11. The VLANs are implemented according to IEEE802.1Q and supports 1500 bytes MTU. The ISP has to set the right MTU-size.
30. RINEX supports IP version 4 ONLY for now. RINEX management will assign and distribute IP addresses to the Customer ISPs/Peers. The customer SHOULD NEVER uses an IP address that has not been given by RINEX management.
31. Each operator has a duty of confidentiality to the other RINEX operators in RINEX affairs.
32. Each operator must provide 24/7 NOC contact details for use by RINEX management.
33. Each operator SHALL not carry any illegal activities through RINEX as per the Laws of the Republic of Rwanda.
34. Any complaints can be referred to in writing (email or hard copy letter) to RINEX management (rw-adm@ricta.org.rw for administrative/management issues or noc@ricta.org.rw for technical aspects/issues).
35. Any operator intending to discontinue RINEX connection service shall inform the RINEX Management three (3) months prior to the planned disconnection date. The disconnection notice should be sent to RINEX management in writing. There shall not be any refund on charges.
36. In the case of non-payment, the RINEX management shall initiate a disconnection procedure immediately as set in section 9.

TECHNICAL SPECIFICATIONS AND REQUIREMENTS

37. RINEX will provide a layer-2 Ethernet switch fabric for interconnection. Each peer will be given a port at the RINEX facility, through which they will peer with other RINEX peers.
38. Each Operator is responsible for providing a circuit to the RINEX facility.
39. The Operator shall announce only those routes that belong to their Autonomous System and their customers.
40. Participants/peers will have to exchange routes with each other without bias or disregard.
41. Every participant/peer will keep its RINEX link connected at all times (24/7) for the purpose of facilitating the efficient routing and interconnection of IP transit networks within Rwanda.
42. Each participant/peer will be provided with a 2U rack space. There might be restrictions in the future when capacity is limited.
43. RINEX management provides to RINEX peers with a Layer-2 Ethernet switch fabric to connect the peers, and BGP route server services.
44. The Operator may only connect equipment that they own and operate themselves at RINEX facility. They may not connect equipment on behalf of third parties.
45. The Operator may only utilize a single Layer-2 MAC address to place a single layer-3 router per port allocated from the TIX switch fabric. This Layer-3 router shall be housed at RINEX facility.
46. It is preferred that each participant/peer have their own Autonomous System number, peers without an ASN allocation will be assigned an ASN from private ASN space by the RINEX

Management.

47. Any participant/peer, who has previously been connected to the RINEX using private ASN and acquires a new public ASN, must notify the RINEX Management as soon as possible in order to incorporate this development into the BGP peering at RINEX.
48. The operators are encouraged to advertise routes of their IP prefixes to the RINEX route servers.
49. The operators shall not advertise routes other than their own routes. Any peer should never advertise other prefixes (third parties) without the prior written permission of the assigned holder of the address space.
50. The operators shall not advertise a “next-hop” other than their own.
51. The peering between routers across RINEX will be via BGP4. Any kind of tunnelling between participants/peers is explicitly forbidden.
52. The operator shall not generate unnecessary route flap, or advertise unnecessarily specific routes in peering sessions with other participants across RINEX.
53. The Operator shall not point their default route to RINEX or any other peer.
54. The operator must, on all interfaces connected to the RINEX switch fabric, disable Proxy ARP, ICMP redirect, CDP, IRDP, directed broadcasts, IEEE802 Spanning Tree, any interior routing protocol (IRP) broadcasts, and any MAC layer broadcasts other than ARP or inverse-ARP.
55. The operator must, on all interfaces connected to the RINEX switch fabric, disable any duplex, speed, or other link parameter auto-sensing.
56. RINEX operators must set netmasks on all interfaces connected to RINEX to include the entire RINEX peering LAN (Currently 196.223.12.0/25)
57. The operators shall avoid congestion on their interfaces or transmission links at or into RINEX so as to not cause unwanted latency for traffic at RINEX.
58. The operators shall not announce ("leak") prefixes including some or all of the RINEX peering LAN to other networks without explicit permission of RINEX.
59. RINEX operators must clearly label all equipment that resides at the RINEX facility with ownership and contact information.
60. RINEX operators will not touch equipment and/or cabling owned by other participants and installed at RINEX or any other equipment in the RINEX facility room without the explicit permission of the participant who owns the equipment.
61. The operator should not routinely use RINEX switch fabric for carrying traffic between his or her own routers, unless specifically granted the permission by RINEX management.
62. The operators will not install traffic monitoring software to monitor traffic passing through RINEX, except through their own ports. RINEX may monitor any port but will keep any information gathered confidential, except where required by law or where the RINEX management has determined a violation of these policies.
63. The operator shall endeavour 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.
64. The operator is responsible for the connection/circuit from the Operator’s headquarters/PoP to the RINEX facility. RINEX facility is hosted in a third-party premise, over which RICTA Management is NOT the authority.

QUALITY OF SERVICE

65. RINEX management will take all necessary precautions to ensure maximum uptime for the RINEX facility; however, it will not provide rebates of any sort for down time.
66. RINEX will run on a non-blocking switching architecture to avoid delays.
67. RINEX management shall ensure proper environment (Proper Air conditioning with Humidity control) at the facility.
68. The Operator shall augment the bandwidth port capacity in the event the utilization of the existing link exceeds 80% of the capacity for 4 hours in a day and for 7 days. Such capacity management shall be through increase of capacity and not through reduction routes announced.
69. RINEX management will ensure that the facility is physically secure and will provide access to its members when needed.

DATA COLLECTION

70. RINEX usage statistics shall be collected in real-time and only the aggregate traffic volume will be published on RINEX website.
71. Any other information collected by RINEX shall be kept confidential subject to any obligation of disclosure in accordance with the applicable laws.
72. RINEX shall comply with the telecommunications law and regulations in Rwanda in respect of any data collected.

DATA ACCESS

73. All members are to ensure that computer data processed or stored on their network intended for public access shall be made available in a manner that does not deny or unduly delays access from other RINEX members.

SERVICE FEES

74. There are two (2) types of fees; the one-time fee and the connection fee referred to as the “RINEX service fees”
75. The operator shall pay the connection fee on an annual basis. RINEX management accepts shall accept quarterly payments if the applicants/peering organization officially request that payment model.
76. This policy covers ONLY fees associated with ports connection at the RINEX Switch. Any other fees, such as, but not limited to, colocation services and/or others, should be dealt with the organization in charge with the hosting facility (in this case, the organization/entity in charge of the Virtual Landing Point – VLP) or the Telecom House Building.
77. The port connection fee is payable in advance.
78. The applicable RINEX Service Fees amount should be as set in the “Pricelist for RINEX”.
79. Failing to pay the port connection fees shall result in disconnection of RINEX connection of the

concerned operator.

80. The Operator pay the fee by either Cash or Pay check at the RICTA Ltd Bank account:
81. Name of the Bank:
82. RICTA Account #:
83. RINEX Management (RICTA Ltd.) shall not provide any kind of refunds for down time. RINEX Management (RICTA Ltd.) shall do its best to ensure the best availability of service.

PORT DISCONNECTION

84. This disconnection procedure shall be initiated:
85. For the non-compliance with the “The Terms & Policies for RINEX”.
86. For the non-compliance with the RINEX Service fees.
87. For issues related to law enforcement or/and National Security.
88. For issues related to the non-compliance with the “Terms & Policies for RINEX”, the operator shall be informed in writing (email and/or hard copy letter) prior to the disconnection. The disconnection should be executed immediately.
89. For issues related to Law enforcement, National Security and/or Cyber security, the operator shall be disconnected with or without formal written notice. The disconnection shall be executed immediately.
90. For issues related to the non-compliance with RINEX Service fees, the operator shall be disconnected on the following working day of the connection service anniversary date.

INSURANCE

91. Members/operators are responsible for the insurance of their own equipment.

LIABILITY FOR OUTAGES

92. RINEX operators using RINEX switch cannot hold the RINEX Management liable for RINEX network/switch fabric outages of any kind.

CHANGE OF THIS POLICIES

93. RINEX Management reserves the right to make changes to these policies, following due consultation with RINEX operators.