THE Nigerian STOCK EXCHANGE

# THIRD PARTY CONNECTION ACCEPTABLE USE POLICY:

## Objective

To ensure that a secure method of connectivity is provided between the Exchange and all Third Parties, and to provide guidelines for the use of network and computing resources associated with Third Party use of the Exchange's technology resources i.e. provide guidelines for anyone whose network and/or computer systems are connected with The Exchange's computer and/or network systems.

Third Parties are anyone whose network and/or computer systems are connected with The Exchange's computer and/or network systems.

## Applicability

This policy applies to all Third Parties (companies, organizations, individuals) who access The Exchange's technology offering through their network and/or computer systems ("Third Party Network") and extends to anyone whom the Third Parties allow to access/use The Exchange's network and/or computer systems.

It is important that this Acceptable Use Policy (AUP) is read carefully by the Third Party. This AUP forms part of the contractual documents between The Exchange and the Third Party. Where there is a conflict between the terms of this AUP and the agreement between the Third Party and The Exchange the terms of this AUP shall supersede the terms of the agreement.

***Definition:*** A Third Party Network is any physical or logical connection between any component of The Exchange's network and/or computer(s) and the terminals or other network components of a Third Party.

Third Parties include companies and organizations who are The Exchange's Vendors, Suppliers, Regulators, Dealing Member Firms or companies with whom The Exchange has collaborations. The defining factor for whether a company, an organization or an individual is a Third Party within the meaning of this AUP is whether the Third Party has a Third Party Network.

Third Party Network connections are to be used only for the specific business purposes intended for each connection. Any violation of this *AUP* may result in immediate termination of the connection with or without notice, and/or the termination of your agreement with The Exchange, with or without notice.

**1**. **Introduction**

1.1 This AUP outlines the principles that govern the actions and conduct of Third Parties who have a Third Party Network.

1.2 The term "User(s)" means whoever has access to and/or uses the Third Party Network and this includes the Third Parties, their employees, customers, clients, service facilitators, service providers e.t.c.

1.3 The terms "you" and "your" means the Third Party.

1.4 This AUP is subject to amendment, modification or substitution at any time. Your continued connection after any such amendment, modification or substitution would mean acceptance of any new AUP.

**2. Enforcement Actions** – *our rights to investigate, suspend, restrict or terminate the connection and agreement.*

We reserve the right to investigate any suspected violation(s) of this AUP. If we become aware of any possible violations, we may initiate an investigation, which may include gathering information from the User involved and/or the complaining party (if any), as well as examine materials on our servers, networks or any other equipment associated with the connection. The Third Party hereby gives its consent to The Exchange to approach, without any recourse to the Third Party, any User to obtain/gather the required information.

We will take action if you abuse the connection or any form of connectivity to The Exchange or use The Exchange's data in an unauthorized manner. The actions we may choose to take at our sole discretion, include but are not restricted to:

(a) A formal warning to you to immediately desist from such activities;
(b) Suspension of your connection, with or without notice;
(c) Restriction of your access to all or any part of our connection, with or without notice;
(d) Termination of your connection, with or without notice;

(e) Termination of your agreement with The Exchange, with or without notice.

**3. Unacceptable Use**

We can assume no responsibility for the content contained on the Internet or otherwise available through the connection. You assume the risk of accessing content through the connection, and neither we nor any of our employees, shall have any liability for any claims, losses, actions, damages, suits or proceedings arising out of or otherwise relating to access to such content.

You are required to use any information that you generate and publish using the connection in accordance with the terms of your agreement(s) with The Exchange and you are solely responsible for any liability which arises to either you or The Exchange if you fail to do so. You must ensure that the recipient of the information that you generate and publish through/from the connection is one allowed under the terms of your agreement (s) with The Exchange and that such recipient does not in receiving or using the information breach either this AUP or the agreement between you and The Exchange.

You must not use the connection or allow anyone who has access to the connection to use the connection in ways that; breach the terms of this AUP or the terms of your agreement with The Exchange, in ways that can be deemed unlawful, illegal or detrimental to the image and brand of The Exchange.

Third Parties are prohibited from carrying out the following activities. The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of Unacceptable Use.

- *Compromising The Exchange's reputation or its relationships with its stakeholders, or embarrassing the Exchange.*
- *Making representations or expressing opinions purporting to be those of The Exchange, without appropriate authority.*
- *Sending, downloading, displaying, printing or otherwise disseminating data and electronic communications that contain threats, defamatory material, pornography, hoax virus alerts, unsolicited commercial or political messages, materials that constitute racial, sexual harassment, chain letters, or communications that promote activities that are otherwise unlawful or improper.*
- *Behaving in a manner that violates rules, regulations or legislative laws applicable at the state, national or international level.*
- *Infringing copyright, trademarks, trade secrets, patents or proprietary rights of The Exchange or third parties' products and services.*

- ❖ *Performing, or attempting to perform, intrusive activities against The Exchange's systems or another entity's computer, electronic communications, or telecommunication systems.*
- ❖ *Distributing malicious or destructive code including, but not limited to, viruses, worms, and spyware or Trojan horses.*
- ❖ *Disclosing one's access credentials, intentionally or unintentionally, to a third party.*

In addition to these, the following shall be observed:

- *Any of The Exchange's equipment located on Third Party premises will only be configured for IP connectivity and will only be used for The Exchange's related data transfers.*
- *Configuration changes on The Exchange's equipment shall only be performed after notification and approval by the appropriate The Exchange personnel.*
- *The password on The Exchange's devices located on the Third Party premises will be set by The Exchange and shall not be changed by the Third Party unless approved by the appropriate Exchange personnel.*
- *The Third Party shall notify the appropriate Exchange personnel when its employee, who has access to any of The Exchange's network resource per The Third Party Network connection, leaves the Third Party or is transferred to another position which no longer requires access.*
- *The Third Party shall assume all responsibility for protection of its private network(s) and/or computer systems which may be interconnected via the Third Party Network connection to The Exchange.*
- *Only employees of the Third Party who have been approved by The Exchange to access the Third Party Network connection shall use the resources associated with the Third Party Network connection.*
- *The Third Party shall notify the appropriate Exchange personnel whenever it wants to change its employees who are to access the Third Party Network, and seek the prior approval of The Exchange for such change.*
- *The Third Party shall notify the appropriate Exchange personnel whenever there is a change in the functional requirements of The Third Party's network and/or computer systems where this impacts the connection provided by The Exchange to the Third Party.*
- *The Third Party shall notify the appropriate Exchange personnel whenever there is a change in the access method used for the Third Party's network and/or computer systems where this impacts the connection provided by The Exchange to the Third Party.*
- *The Third Party shall timeously rectify any shortcomings, weaknesses and/or gaps in the Third Party's network and/or computer systems identified by internally generated audit reports and audit reports provided by The Exchange. Where the shortcomings, weaknesses and/or gaps are*

*identified by an internally generated audit report the Third Party shall promptly notify the appropriate Exchange personnel of such shortcomings, weaknesses and/or gaps.*

- *The Third Party shall provide timely and adequate assistance, documents and information to The Exchange's personnel in the investigation and resolution of any security incidents or issues relating to the Third Party Network connection.*

## 4. Your responsibilities – Security

You are responsible for the security of the connection. The Exchange is not responsible for the consequences of your failure to employ adequate security measures (e.g. lost or corrupted files, identity theft, and fraud).

You are responsible for the security of the devices that are directly or indirectly connected to the Third Party Network. This includes, but is not limited to: PCs, iPods/iPads (or equivalent), laptops, smart-phones, wired and wireless networking devices.

If we observe that devices on your end of the connection cause significant impact to our service or form part of a "botnet" (machines hijacked by others to distribute malicious software or other forms of abuse), we reserve the right to suspend or terminate your connection without notice.

You must ensure that your devices are protected with up-to-date anti-virus software and a properly configured firewall as a minimum where applicable.

You must keep your password(s) confidential and secure. If you think that your password(s) has become known to any unauthorized person or may be used in an unauthorized way you should immediately notify the appropriate personnel of The Exchange of this occurrence and also immediately take steps to change your password. If you believe that any of your devices have been used to breach the terms of this AUP you must inform us immediately.

I