THE NIGERIAN STOCK EXCHANGE

CONFIDENTIAL DATA POLICY

Table of Contents

1.0 Introduction

This policy provides general guidelines on protecting The Exchange's corporate information classified as confidential according to the terms of the agreement with The Exchange, from unauthorized disclosure. Specifically, it reduces the threat posed to corporate information by theft and mishandling of data.

Effective implementation of this policy would ensure the following:

- Protection of The Exchange's confidential information whether in transit or at rest.
- Demonstrate that The Exchange is taking corporate responsibility for data in its care.

2.0 Purpose

The purpose of this policy is to set guidelines to prevent unauthorized disclosure of information by laying down clear standards of practice to maintain good security where confidential data is involved.

3.0 Scope

This policy applies to information classified as 'Confidential' according to terms of the agreement between The Exchange and a contractor, vendor, consultant or agent handling information at/of The Exchange either in paper form or electronic format.

4.0 Policy

All stored information, i.e. data, should be assigned an owner with the responsibility to protect and control access to the data. When data is classified as confidential, extra care must be taken to protect it either at rest or during transmission. Appropriate technical and organizational measures should be taken against unauthorized access, accidental loss, destruction of, or damage to, confidential data.

4.1 Storing & Disposal of Confidential Documents

- All information classified as confidential must be kept secure at all times.
- Paper based information may be stored in file cabinets, and in locked offices, or in designated areas where physical controls are in place to prevent disclosure when not in use.
- Confidential data in electronic format must be stored in appropriate media that have adequate technologies to protect it at rest. Such techniques may include encryption and well defined access controls.
- Confidential data in electronic format must be backed up regularly and tested to prevent data loss due to corruption when encrypted.
- Access to confidential data (paper and system held) must be verified against an established access control matrix to prevent unauthorised disclosure and circumvention.
- Access to confidential data (paper and system held) must be logged and documented.
- Confidential data (paper or system held) should be periodically reviewed to ensure that the information is accurate, up to date and complete.
- Confidential data (paper and system held) should be kept in line with the terms of the agreement with The Exchange.
- Confidential information must be disposed of securely and must be done in line with the terms of the agreement with The Exchange. Documents should not be printed off but read on the screen as practical as possible.

4.2 Handling and Transmission of Confidential Data

- Data residing on laptops, USB sticks or back-up tapes and the likes must be encrypted to mitigate data loss due to theft.
- Always exercise due care when handling confidential information and shield the information from disclosure while handling or processing on a computer.
- A contractor, vendor, consultant or agent shall ensure that its staff who do not have relevant authorization to access computer or paper records belonging to The Exchange are prohibited from accessing them and that sufficient controls are put in place to ensure compliance with this provision.

4.2 Disclosure

- Care must be taken to ensure any disclosure of confidential information is for an authorised purpose.
- A request to access/view confidential information should be authorised by the representative which is recognised under the terms of the agreement with The Exchange.
- There may be occasions when the court, regulator and/or law enforcement agencies may ask for the release of confidential information disclosures shall not be made except in line with the agreement with The Exchange.

5.0 Monitoring & Enforcement

A contractor, vendor, consultant or agent found to have violated this policy may have its agreement with The Exchange terminated, with or without notice.