THE NIGERIAN STOCK EXCHANGE

ACCESS CONTROL POLICY

Table of Contents

1.0 Introduction

Proper access control is critical to maintaining an effective security structure and to the provisioning of a safe, secure and readily accessible environment in which to work. The Exchange implements appropriate levels of access controls across its Information systems and services in order to provide authorized, granular and appropriate user access, and to ensure the preservation of data confidentiality, integrity and availability in accordance with the Information Security Management Policy.

Effective implementation of this policy would ensure the:

- Prevention of unauthorized disclosure or theft of information, fraud and possible litigation
- Institute the correct use and management of access controls throughout The Exchange, thereby protecting the interest of the Exchange and its staff.

2.0 Purpose

The purpose of this policy is to define a framework to guide the correct use and management of access creation and access control in order to allow authorized users access appropriate data and resources and deny access to unauthorized users.

3.0 Scope

This policy applies to all Exchange employees, contractors, vendors, stock brokers, agents and visitors, and it takes precedence over all other relevant policies or procedures that may be created on access control. This policy covers the following:

- All Exchange Information Systems and Networks;
- All users and use of The Exchange's Information Technology Resources, Information Systems and Network;
- All connections to The Exchange network (locally or remotely);
- All connections made to external networks through The Exchange's network.

By accessing any Information System resources which is owned or leased by The Exchange, users are agreeing to abide by the terms of this policy.

4.0 Policy

This policy provides guidance on restricting access to The Exchange's information and information assets by providing the blueprint for the management of user access, authorizations and control mechanisms applicable to computer networks, operating systems, databases, applications and information. These restrictions are guided by business and regulatory requirements and it protects The Exchange from security threats such as internal and external intrusions.

4.1 Principles of this Policy

- Logical access and other necessary information shall be provided to employees and other users to carry out their responsibilities effectively and efficiently.
- Login IDs shall follow an identifiable pattern and will be unique. It shall segment staff, agents and contractors and visitors based on functional requirements and in-line with The Exchange's nomenclature. The login ID shall not provide information on the user's description or functions.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient controls on access are in place.
- User accounts shall be created or deregistered only through a formal request using The Exchange's approved processes and appropriate forms. New employee access or employee de-registration can only be approved by the Head, Human Resources and Head, Information Security. Other requests may be submitted for approval by Heads of Departments.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the head of the appropriate department and Information Security Department.

- Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights to operating systems, network, database or applications will be allocated based on the principles of least privilege and need to know.
- Every user should endeavour to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accordance with the data's classification, and are consequently responsible for ensuring that data security, confidentiality, and integrity are maintained.

4.2 Access Control Authorization & Methods

- Access to The Exchange's Information Technology resources and services will be given through the provision of a unique account and complex password on the appropriate platforms where access is required.
- Access to IT resources and services will not be provided without prior authentication and authorization of a user's Exchange Windows Active Directory account.
- User and service account passwords must comply with The Exchange's password policies and these passwords shall be managed using The Exchange's approved service delivery methods.
- Access to confidential, restricted or protected information will be limited to authorized persons whose job responsibilities require it, as determined by the data owner or their designated representative, and as stipulated in the Confidential Data Security Policy.
- Requests for access permission to be granted, changed or revoked must be made formally through approved processes using the appropriate forms.
- Access for remote users shall be subject to authorization by both Information Technology and Information Security, and shall be provided in accordance with the relevant Exchange policies. No uncontrolled

external access shall be permitted to any network device or networked system.

- Groups of information services, users and information systems must be segregated on networks.
- The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system.
- Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system.
- Information systems managing data of a sensitive nature must have an isolated dedicated computing environment.
- User activities involving confidential or protected data shall be logged and preserved according to data retention policies.
- Access to data should be controlled according to the data classification levels described in the Data Classification Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, SELinux, RBAC mechanisms provided in operating systems, user account privileges, server and workstation access rights, firewall permissions, RADIUS/TACACS+ based AAA systems, IIS intranet/extranet authentication rights, database rights, isolated networks and other methods as necessary.

4.3 Mobile Computing

- Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.
- User identifiers and user credentials must be protected to reduce the risk of unauthorized access to information and information technology assets. In particular, users must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places.
- Where remote access services are used, mobile devices should be configured to prevent its use as a conduit between the non-Exchange and Exchange networks (e.g., VPN split tunnelling must be disabled).

- Network access to mobile devices from non-Exchange networks must be blocked by implementation of firewalls or filtering technologies to protect against attack
- Mobile devices must be protected against mobile and malicious code.
- Mobile devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

5.0 Responsibilities

- Users are expected to become familiar with this policy and abide by The Exchange's policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- System, application, database, and network administrators are expected to be familiar with this policy and comply with it.
- Information owners and custodians are required to ensure that access controls mechanisms are implemented correctly and accesses are duly authorized as provided by this policy.
- Information Security Department is expected to perform regular independent reviews and assessments to ensure that this policy is being adhered to.

6.0 Monitoring &Enforcement

6.1 Access Control Monitoring and Review

- A formal process should be conducted at regular intervals by system owners and data owners in conjunction with the Technology department to review users' access rights.
- The review should be logged and the Technology department should sign off the review to give authority for users' continued access rights or revocation of any redundant access.
- Relevant system and database events should be logged, including unsuccessful logins, alerts from intrusion detection systems and firewalls. These logged details should include date, IP address, User-IDs, and the action performed.

6.2 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action. Penalties for non-adherence to this policy will depend on the seriousness of the offence, and will be in accordance with The Exchange's disciplinary procedures.

Any contractor, vendor, stock broker, agent and visitor found to have violated this policy may have its/his/her agreement with The Exchange terminated with or without notice.

6.3 Terminology

NTFS	- New Technology File System
SELinux	- Security Enhanced Linux
RBAC	- Role-Based Access Controls
TACACS+	- Terminal access controller access control system.

AAA	- Authentication, Authorization, and Accounting
IIS	- Internet Information Server