SEC NIGERIA
SECURITIES AND EXCHANGE COMMISSION, NIGERIA

EXPOSURE OF PROPOSED GUIDELINES ON MINIMUM OPERATING STANDARDS FOR INFORMATION TECHNOLOGY FOR CAPITAL MARKET OPERATORS (CMOS)

Preamble

This document sets out the Minimum Information Technology Operating Guidelines for CMOs in the Nigerian Capital Market. The provisions apply to all categories of CMOs unless in sections where reference is otherwise made to specific CMO categories.

The purpose of the Guidelines is to establish a threshold of operational efficiency in the Nigerian Capital Market through the effective adoption of Information Technology in driving business operations and ensuring the security, confidentiality, integrity and reliability of Information Systems.

1. Computing Environment

This refers to the collection of electronic workstations, data storage devices, computer machines, software applications and networks interacting together to support the processing and exchange of electronic information for the business.

1.1 Requirements for Computing Environments

i. The computing environment shall be any or a combination of Client-Server, Cloud, Distributed or Time-Sharing environments.

ii. The computing environment shall be such that is well suited to the operations and business objectives of the Capital Market Operator (CMO).

iii. The hardware systems and all other IT infrastructure in the environment shall be located in physical spaces with adequate security, access control, power and cooling to ensure service availability and continuity.

1.2 Requirements for Private Data Center, Colocation and Public Cloud Service

Capital Market Operators are required to either own and manage a private data centre, rent rack spaces in a colocation data centre facility, or employ the services of a public cloud service provider (CSP) for their computing, storage and networking requirements. A hybrid of any of these can also be employed.

i. Requirements for CMOs that utilize Private Data Centers

(a) The physical space shall be adequate to house all the servers, storage devices, networking devices and computer machines in well-arranged racks with room for scalability.

(b) There shall be a biometric access control system in place for authorized entry into the data center
(c) There shall be a round-the-clock monitored video surveillance of the data center using CCTV devices. This shall provide a good view of the entry point and of all critical devices in the data center.
(d) The data center shall be up to the standard of a Tier-3 rated facility in terms of expected uptime, fault tolerance and redundancy, and multiple paths for power and cooling.
(e) There shall be adequate personnel and infrastructure in place to ensure physical security.
(f) There shall be a well-trained and qualified data center administrator to manage the facility.

ii. Requirements for CMOs that utilize Colocation services

Adequate due diligence shall be carried out before subscribing to the service of a colocation data center facility. The following minimum requirements shall be in place for a colocation data center facility to be used by CMOs:

(a) The colocation data center shall be up to the standard of a Tier-3 rated facility in terms of expected uptime, fault tolerance and redundancy, and multiple paths for power and cooling.
(b) The location shall be reasonably close geographically to the CMO's headquarters and shall provide ease of access for IT personnel who would need to visit for regular or emergency maintenance.
(c) They shall have a verifiable track record of reliability in terms of adequacy of power and cooling, data backup, low-latency networking, adequate bandwidth and physical security.
(d) There shall be a well-executed service level agreement that reflects fair pricing for the service received and clearly stated rights and obligations of both parties. This shall meet up to the applicable ISO standards for Service level agreements (SLA) ISO/IEC 19086-1:2016 or comparable international SLA standards.
(e) They shall demonstrate compliance with the rules of NITDA and any other relevant government agencies

iii. Requirements for CMOs that subscribe to Cloud Services

Adequate due diligence shall be carried out to properly assess a CSP before subscribing to their service. The CSP shall have proven capacity to provide any of the cloud service models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-

service (IaaS). The following minimum requirements shall be in place for a CSP to be used by CMOs:

(a) The CSP shall demonstrate adherence to industry best practices and compliance with the rules of NITDA and any other relevant government agencies.

(b) The CSP shall possess certifications like the ISO 27000 series for information security or comparable international information security standards and comply with other applicable and recognized international standards and frameworks.

(c) The CSP's data security, data governance and business policies must be well understood and must align with the CMO's data security policies and business processes. The CMO must be aware of the regulatory and data privacy rules governing personal data in the jurisdiction of data residency being used by the CSP and the CMO shall ensure this aligns with its business processes and objectives.

(d) There shall be a well-executed service level agreement that reflects fair pricing for the service received and clearly stated rights and obligations of both parties. This shall meet up to the applicable ISO standards for Service level agreements (SLA) ISO/IEC 19086-1:2016 or comparable international SLA standards.

1.3 Requirements for Servers, User Systems, Workstations, Storage/Backup Systems

Depending on the type of computing environment adopted, the following guidelines specify the minimum requirements that shall apply for the management of the hardware and software of various computer systems that CMOs may use to support their operations.

i. General Requirements for Computer Machines

(a) The hardware and software components of all computer machines shall be adequate to meet the computing needs of the CMO.

(b) For all computer hardware, the depreciation standard shall follow an established depreciation policy which must require that only fully functioning computing machines are being used in the enterprise.

(c) All software in production shall be such as are still being supported in terms of regular service update (patches) by the software provider.
(d) There shall be a storage management plan in place that defines the usage threshold for storage disks to ensure there is always adequate storage space to prevent unexpected failure of systems and applications.
(e) There shall be a backup management plan in place that includes a scheduled daily incremental backup of critical data and replication to an offsite backup facility. There shall also be regular scheduled test recovery exercises to ensure completeness and correctness of data backup.

ii. **Servers**

(a) The servers shall run on a minimum of Microsoft Windows Server 2016 operating system or the equivalent UNIX/Linux and comparable server operating systems. All operating system versions in use shall be licensed, activated and still be fully supported by the OEMs in terms of regular receipt of security updates and patches. All installed software applications shall be such as are licensed and compatible with these minimum operating system versions.
(b) The server hardware shall meet the minimum hardware requirements for installing a Microsoft Windows Server 2016 operating system or the equivalent UNIX/Linux and comparable server operating systems.

iii. **User Systems**

(a) The user desktop and laptop computers shall run on a minimum version of Microsoft Windows 10 Pro or equivalent Apple, and comparable operating systems. All installed applications shall be such as are licensed and compatible with these minimum operating system versions.
(b) The hardware requirements for desktop and laptop computers shall meet the minimum requirements for installing a Microsoft Windows 10 Pro as operating system for desktops and laptops.
(c) The USB ports on the system shall be configured to ensure that official documents cannot be moved or copied out of systems to unauthorized locations. Alternative methods to ensure this can also be employed.
(d) There shall be adequate power supply and backup in place to ensure users can work on their computers uninterrupted.

2. Information Technology/Information Systems Management and Governance

Information Systems refer to the CMO's sociotechnical system for the collection, storage, processing and transmission of information and other digital products. While IT systems speak to the hardware, software and networks that underlie the operation of Information Systems. Based on this context, the minimum IT/IS management and governance requirements set out here, indicate the minimum requirements for the management (i.e. monitoring and administration) of IT/IS and the governance of IT/IS; i.e. the methodology for oversight to enable the alignment of IT/IS operation to organizational strategy. This section (2.1 to 2.4) does not apply to CMOs classified as Capital Market Consultants/Experts, Sole Proprietorships or Business Names.

2.1 Requirement for IT Policy

i. There shall be an IT policy duly approved by the Board and shall be reviewed in not more than every five years. It shall set out the organisation's policy for the management and governance of IT and Information Systems.

ii. The IT policy scope shall comprehensively reflect and comply with the minimum guidelines set out in this document and shall cover every other area as are relevant to ensuring information security and the efficiency of technology dependent business processes.

iii. There shall be in place, an IT steering committee constituted by the board and chaired by an Executive Director to provide IT/IS governance for the organisation. The steering committee shall meet regularly; at least monthly.

2.2 Requirement for IT/IS Audit and Risk Management

i. There shall be an internal IT/IS audit function in place and the audit approach shall be risk-based.

ii. There shall be an IT/IS risk management function in place. This shall be a standalone function or part of an enterprise-wide risk management function.

2.3 Requirements for Information Security and Cybersecurity

i. There shall be an Information Security and Cybersecurity policy in place and it shall form part of the enterprise IT policy of the organisation.

ii. The Information Security and Cybersecurity policy shall conform to up-to-date international best practices and shall be appropriate and adequate to ensure the safety, confidentiality and reliability of the

network, data, information systems and their underlying technologies.

iii. Firewalls, intrusion detection technologies, data encryption, and other relevant technologies and systems shall be employed to provide adequate network security against cybersecurity threats.

iv. All user systems (Computers and hand-held devices) hosted on the network shall be secured with up-to-date antivirus and antimalware protection.

v. There shall be a policy in place to guide acceptable access and use of information systems remotely to ensure adequate security, confidentiality, reliability and integrity of data, network resources and information systems.

vi. Physical access to network infrastructure, workstations and critical systems shall be restricted to only authorized persons. Strict access control policies shall be in place and shall be followed. This shall include password policies that require multi-factor authentication and use of passwords with adequate complexity.

vii. IS and Cybersecurity policies shall be communicated to all staff of the organisation with the roles of technology users in ensuring the security of the enterprise clearly spelt out.

viii. There shall be regular and updated security awareness for all staff in the organisation, communicated via email and other media.

ix. For Exchanges, Fund Managers, Registrars, CSDs and Clearing Houses, regular penetration tests shall be conducted at least annually to detect vulnerabilities and check the resilience of the network and systems to threats and malicious activities. The tests shall be conducted by a certified and trusted third party service provider and the results of the tests shall be documented securely within the organisation. There shall also be documentary evidence that identified threats and vulnerabilities are adequately taken care of within a reasonable time frame.

2.4 Requirement for IT/IS Staff

i. All IT/IS functions shall be duly manned by qualified and competent persons with verifiable certification, relevant education or cognate experience as required. A minimum of BSc/HND or the equivalent is required for the handlers of IT/IS management functions.

ii. IT/IS staff shall be adequately trained to keep pace with the quick changes and evolutions characteristic of the technology space.

iii. Staffing shall be designed to ensure there are always alternates for sensitive roles. Key-man risks and other skills gaps shall be avoided.

3. Web Sites and Electronic Mails

The following guidelines on websites and emails apply to all CMOs. However, requirements in section 3.1 (v to ix) do not apply to CMOs classified as Capital Market Consultants/Experts, Sole Proprietorships or Business Names.

3.1 Web Sites

i. All CMOs are required to have a functional website
ii. Websites shall contain correct, up-to-date, and relevant information. Websites shall not display errors or system messages revealing information about the underlying configuration of web applications.
iii. Websites shall use the HTTPS (not merely HTTP) network protocol and other measures to ensure secured interoperability
iv. Adequate security measures must be put in place to ensure protection against availability attacks (especially denial of service attacks), integrity attacks and confidentiality attacks.
v. Regular audits and vulnerability tests shall be conducted to identify and fix vulnerabilities in the underlying operating systems, databases, webservers and third party software/applications.
vi. Applicable system and web application updates (patches) shall be regularly applied once they become available.
vii. Access to databases and backend systems shall only be possible through front-end web applications and not directly from the internet, and shall only accord minimal privileges to databases and back-end systems.
viii. Websites that allow file upload shall verify file types and scan for malicious code.
ix. The content management of websites shall be entirely domiciled in the CMO and not a third party.
x. The development, hosting and maintenance of websites can involve third parties, in which case all the applicable requirements stated in this document to ensure availability, confidentiality and integrity of the website shall be included as mandatory elements of the terms of contract and SLA.

3.2 Requirements for Electronic Mails

i. All CMOs are required to have a functional electronic mailing system either hosted privately or using a cloud service provider.
ii. Domain names shall be owned and registered by the CMO. Use of the services of free email providers and private emails like Yahoo

mail, Gmail, Hotmail, etc. is not acceptable for official communications.

iii. In setting up the email service, appropriate encryption protocols must be applied to achieve a minimum of transport-level encryption for securing email content.

iv. There shall be an email system security management plan in place to ensure mail server and content security, security of the operating systems, security of mail gateways and mail client security.

v. Email users shall be trained on how to prevent email client-side attacks like spoofing and phishing.

4. IT Business Continuity and Disaster Recovery

CMOs shall have a documented Business Continuity plan and a Disaster Recovery plan. This is to ensure that CMOs can continue operations at an acceptable level in the event of unforeseen IT service disruptions. This section (4.1 & 4.2) does not apply to CMOs classified as Capital Market Consultants/Experts, Sole Proprietorships or Business Names.

4.1 Requirements for Business Continuity (BC)

i. Business Continuity plans shall be up to the standard of international best practices. The plans shall include identification of critical business functions, key personnel, and backup site and other elements that ensure the continued operation of IT systems supporting critical functions of the organisation.

ii. There shall be regular (at least annual) testing of the BC plan to confirm that operations and critical services are uninterrupted in the event of unforeseen disruptions.

iii. There shall be documentary evidence that BC tests are conducted as scheduled and that necessary adjustments are made to fix identified gaps.

4.2 Requirements for Disaster Recovery

i. Disaster Recovery plans shall be up to the standard of international best practices. The plan shall include elements of business impact analysis, assumptions and constraints, communication processes, data and system backup plan, damage and impact assessment, response communication and action plan.

ii. There shall be regular (at least annual) testing of the DR plan to confirm that IT services can be restored from a DR site in the event of a disaster.

iii. There shall be documentary evidence that DR tests are conducted as scheduled and that necessary adjustments are made to fix identified gaps.

5. Additional Technology Requirements for CMO Categories

5.1 Exchanges

i. All Exchanges shall have secure trading platforms with robust features that include real-time quotes, charting tools, news feeds, trade monitoring and premium research.

ii. All Exchanges shall have a surveillance system that provides real-time monitoring of all trading activities.

5.2 Fund/Asset Managers

The following addition requirements are aimed at improving accessibility to the market for retail investors and to drive market penetration and inclusion.

i. Fund/Asset Managers are required to have websites and web applications that allow investors to securely create and manage investment accounts online, make enquiries using chat-bots or other interactive programs from web browsers.

ii. Fund/Asset Managers are required to have mobile applications that provide free access to the full stack of their service offering and allow retail investors to securely create and manage investment accounts online, make enquiries and receive in-app customer support.

5.3 Brokers

The following addition requirements are aimed at improving accessibility to the market for retail investors and to drive market penetration and inclusion.

Brokers are required to have websites and web applications that allow investors to securely create and manage their equities accounts online, make enquiries and receive customer support using chat-bots or other interactive programs from web browsers.

5.4 Registrars, Central Securities Depositories and Clearing Houses

i. Central Securities Depositories and Clearing Houses shall have databases integrated with APIs that Registrars and Brokers can feed from as approved by the SEC.

ii. Registrars, Central Securities Depositories and Clearing Houses are required to have websites and web applications that allow investors to securely create and manage their profiles online, make enquiries and receive customer support using chat-bots or other interactive programs from web browsers.

5.5 Custodians and Trustees

Custodians and Trustees are required to have websites and web applications that allow their clients to securely create and manage their accounts online, make enquiries and receive customer support using chat-bots or other interactive programs from their web browsers.

Justification: *Given the increased dependence of financial services and related business operations on technology, there is urgent need for the Commission to put in place rules that define the minimum operating standards for the use of information technology by all operators in the capital market. This will help operators harness the huge operational benefits derivable from the adoption of technology and also manage the attendant cybersecurity threats and other risks that accompany the use of technology. It would also positively impact on the effectiveness and efficiency of the Commission to monitor and regulate all CMOs in the market.*

The urgency of the timing of this is also important as sister regulators in other jurisdictions like the US SEC have put in place rules and guidelines that define the use of technology and cybersecurity risk management for different categories of operators.

The draft guidelines specifically define the minimum standards of the use of technology that if adhered to would serve to nudge all CMOs and indeed the entire capital market on the path of operational and regulatory efficiency and effectiveness as well adequately manage the associated risks of using technology.