THE Nigerian STOCK EXCHANGE
RC: 2321

RULEBOOK OF THE NIGERIAN STOCK EXCHANGE, 2015
PROPOSED AMENDMENTS TO ~~DEALING MEMBERS'~~ / TRADING LICENCE HOLDERS' RULES

PROPOSED CYBER SECURITY FRAMEWORK & RULES FOR ~~DEALING MEMBERS~~ / TRADING LICENSE HOLDERS

Definition of Terms[1]

Access Control	The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.
Anti-Virus	A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents, sometimes by removing or neutralizing the malicious code.
Availability	Quality or state of being accessible and usable as expected upon demand.
Confidentiality	State of privacy and non-disclosure of specific information, processes, systems, or devices .
Critical Operations	Any activity, function, process, or service, the loss of which, for even a short period of time, would materially affect the continued operation of a ~~Dealing Member~~ Trading License Holder, its participants, the market it serves, and/or the broader financial system.
Cyber	Refers to the interconnected information infrastructure of interactions among persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.
Cyber Event	An observable occurrence in an information system or network.
Cyber Resilience	A ~~Dealing Member~~ Trading License Holder's ability to anticipate, withstand, contain, and rapidly recover from cyber-attacks.
Cyber Threats	A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a ~~Dealing Member~~ Trading License Holder's systems, resulting in a loss of confidentiality, integrity or availability.

[1] All definitions, except where indicated, were obtained or modified from the glossary provided in the CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016.

Encryption[2]	Converting data into a form that cannot be easily understood by unauthorized people.
Information Asset	Any piece of data, device or other component of the environment that supports information technology-related activities. In the context of this framework, information assets include data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services.
Integrity	Quality or state of completeness, and not having been modified in any manner or destroyed, without authorization.
Malware	Malicious software used to disrupt the normal operation of an information system in a manner that adversely impacts its confidentiality, availability or integrity.
Patch[3]	A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.
Principle of Least Privilege[4]	The principle that users and programs should only have the necessary privileges to complete their tasks.
Ransomware	Malware that requires the victim to pay a ransom to access encrypted files.

1.0 Cyber Security Policy

1.1 The practices and procedures stipulated in this Framework are the minimum requirements for a ~~DMF~~ TLH's effective cybersecurity policy. ~~DMF~~ TLHs may adopt more robust controls and procedures compatible with their Information Technology infrastructure secured in line with their business needs.

1.2 Each ~~DMF~~ TLH shall develop a comprehensive cybersecurity policy which shall:

a. be reviewed and approved by the ~~DMF~~ TLH's Board of Directors (The Board);
b. be subsequently reviewed by the Board at least annually with the view to

[2] Definition from the National Initiative for Cybersecurity Careers and Studies glossary (https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#E)
[3] Definition from the computer security resource centre of the National Institute of Standards and Technology https://csrc.nist.gov/glossary/term/patch
[4] Definition from the computer security resource centre of the National Institute of Standards and Technology https://csrc.nist.gov/glossary/term/Principle_of_Least_Privilege

strengthen and improve its cyber security framework;

c. establish a reporting procedure to facilitate investigation and communication of unusual activities and cyber-attacks to the Board in a timely manner; and

d. cover the core functions of this Framework and be included as a section in the information security policy of the ~~DMF~~ TLH.

2.0 The Cybersecurity Framework Core Functions

Each ~~Dealing Member~~ Trading License Holder firm (~~DMF~~ TLH's) Cybersecurity Framework shall consist of and address the following concurrent and continuous functions:

2.1 Identification – ~~DMF~~ TLHs shall develop their organizational understanding on the existence of – and how to manage – the risk of cybersecurity attacks on their systems, assets, data and capabilities[5]. Examples within this function include: asset management, understanding the business environment, IT governance, and cyber risk management strategy.

2.2 Protection – ~~DMF~~ TLHs shall limit and contain the impact of potential cybersecurity incidents and implement the appropriate safeguards to ensure delivery of critical operations. Examples within this function include: access control, data security, information protection processes and procedures, maintenance, and protective technologies such as regularly updated firewalls, database activity monitoring tools, intrusion detection & prevention system, antivirus solution and email filtering at the gateway.

2.3 Detection – ~~DMF~~ TLHs shall put systems in place for timely discovery of cybersecurity events which may affect the ~~DMF~~ TLHs, and assist them to develop and implement appropriate activities to identify the occurrence of such cybersecurity events. Examples within this function include: anomalies and events procedures, as well as monitoring and detection processes.

2.4 Response –~~DMF~~ TLHs shall minimize the impact of a potential cybersecurity event by developing and implementing appropriate activities to address a detected cybersecurity event. Examples within this function include: response planning, communications, analysis, mitigation and improvements.

2.5 Recovery – ~~DMF~~ TLHs shall make arrangements for timely return to normal operations so as to reduce any adverse impact experienced from a Cyber Event, by

[5] NIST, *Framework for improving critical infrastructure cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

developing and implementing appropriate activities to maintain Cyber Resilience, and to restore any capabilities or services that were impaired due to a cybersecurity event. Examples of activities and expected outcomes within this function include: recovery planning, improvements and communications.

3.0. Identification

a. Threat modeling and risk assessment shall form the basis of ~~DMF~~ TLHs' identification methodology. Priorities for organizational mission, objectives, and activities shall be established along with dependencies and resilience requirements for delivery of critical services, and cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders[6].

b. ~~DMF~~ TLHs shall endeavor to understand and manage all legal and regulatory requirements regarding cybersecurity, including data protection, privacy and ensure that necessary cybersecurity roles and responsibilities are properly assigned and coordinated (for internal and external partners) as follows:

3.1 Governance – Information Security Officer

a. The ~~DMF~~ TLH's Board has the responsibility to oversee the appropriate management of the ~~DMF~~ TLH's cybersecurity risks.

b. The Executive Management of the ~~DMF~~ TLH shall appoint an Information Security (IT Security) officer[7] or IT firm, which shall be responsible for the implementation of the board-approved cybersecurity policies, and define the responsibilities of its employees, outsourced staff, and employees of vendors, and consultants who may have privileged access to or use the ~~DMF~~ TLH's systems and networks.

c. The board or the board Committee overseeing Risk Management shall ensure that the IT Security Officer or IT firm reports on the status of the ~~DMF~~ TLH's cyber resilience and cybersecurity preparedness on a quarterly basis; and The Exchange shall be provided with a copy of the report within 2 (two) business days of its request.

d. The IT Security Officer or IT firm's reports shall include details of the firm's current IT, cyber security and cyber resilience capabilities, and plans to strengthen the ~~DMF~~ TLH's cyber resilience. The reports shall form part of the deliberations of the board or board committee overseeing Risk Management.

3.2 Critical Information Assets- Information Technology Asset Register

[6] Including suppliers, customers, partners.
[7] This can be the Information Technology Officer or Chief Risk Officer who is required to have attended the necessary cybersecurity trainings for this role

a. ~~DMF~~ TLHs shall identify critical information assets comprised of data, hardware, software, systems and facilities as well as relevant personnel based on their sensitivity and criticality for business operations, services, data management and risk strategy as determined by the ~~DMF~~ TLH. Information assets shall be catalogued and prioritized based on their classification, criticality, and business value.

b. ~~DMF~~ TLHs shall develop and maintain an Information Technology (IT) asset register that contains the following information:

(i) hardware systems and ~~DMF~~ TLH personnel to whom these have been issued to,
(ii) software platforms, applications and information systems ,
(iii) details of ~~DMF~~ TLH network resources and critical infrastructure, and
(iv) connections to ~~DMF~~ TLH network and data flows.

c. ~~DMF~~ TLHs shall also ensure that physical information assets are appropriately tagged and captured in the IT asset register.

3.3 Risk Management Strategy

a. ~~DMF~~ TLHs shall establish effective cyber risk management processes, managed and agreed to by the ~~DMF~~ TLHs Board and Management to determine and clearly express the ~~DMF~~ TLH's risk priorities, constraints, risk tolerances, and assumptions which shall be used to support its operational risk decisions.

b. ~~DMF~~ TLHs shall carry out bi-annual risk assessments to identify and understand cybersecurity risks (threats and vulnerabilities) to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, along with the likelihood of such threats manifesting and the impact of such risks on the business. Based on these assessments, the ~~DMF~~ TLH shall deploy controls commensurate to the criticality of the identified risks.

c. The IT Security Officer or IT firm shall ensure that cyber security incidents are brought to the attention of the Board or Board Committee overseeing Risk Management in line with the ~~DMF~~ TLH's board approved incident management policies.

4.0 Protection

Measures aimed at safeguarding the ~~DMF~~ TLH's information systems to ensure delivery of critical services shall include:

4.1 Access Control

~~DMF~~ TLHs shall ensure that:

a. Identities and credentials for authorized devices and all users are carefully managed.

b. Access to critical systems is restricted to authorized individuals based on the principle of least privilege. Where outsourced staff and visitors are granted access to critical systems, ~~Dealing Member~~ Trading License Holders shall ensure that every instance is recorded and properly supervised by authorized employees.

c. Authorized access is granted for a defined purpose, location, and period using strong authentication mechanisms.

d. Physical access and user rights to critical systems are immediately revoked and disabled upon the termination/resignation of staff/authorized user and other instances where access is no longer required or permitted.

e. Strong passwords consisting of at least eight (8) characters including alphanumeric and special characters as well as upper and lower cases are used. All passwords should be changed after thirty (30) days but not later than sixty (60) days.

f. Critical systems and applications accessible over the internet have multi factor authentication.

g. Adequate encryption methods are used for applications connected to the internet to protect sensitive information.

h. Admin or privileged user actions are monitored/supervised and requisite controls are put in place to - limit the number of admin users, restrict access to system logs in which activities are captured, etc.

i. Use of the internet is controlled especially with regard to access to sites that can compromise the security of the ~~DMF~~ TLH's network; and that procedures are established to block malware, and prevent access to suspicious or compromised sites.

j. Server rooms/data centers are secured and monitored by deploying physical, human and procedural/system controls such as the use of security guards, closed-circuit television (CCTV), card access systems etc. where appropriate.

k. Server rooms/ data centers do not have external facing windows and are not located in an area prone to public exposure, exposure to the elements, natural disasters, or unauthorized access.

l. Server rooms/ data centers maintain the required levels of cooling, humidity, etc.

m. Users on applications and systems are uniquely identified and their actions logged for audit trail purposes. Such logs shall be maintained and kept in line with applicable data retention Rules of The Exchange[8]

4.2 Network Security Control

~~DMF~~ TLHs shall provide adequate network security controls by ensuring that:

a. All local area network (LAN) and wireless networks (WN) are properly secured and that security configurations are consistently applied to operating systems, databases, network devices and enterprise mobile devices.
b. Network security devices such as firewalls, proxy servers, intrusion detection and prevention systems are installed, to safeguard their IT infrastructure from internal and external cybersecurity threats.
c. Adequate controls such as anti-virus and anti-malware software are deployed to address virus, malware and ransomware attacks.

4.3 Data Security

~~DMF~~ TLHs shall ensure that:

a. The confidentiality of critical data is not compromised during the process of storing, exchanging and transferring information with external parties. ~~DMF~~ TLHs are required to ensure that critical data (i.e. data-at-rest and data-in-transit) is protected and encrypted using strong encryption methods to prevent unauthorized access, alteration, duplication or transmission.

b. Only authorized data storage devices are allowed within their IT infrastructure through appropriate validation processes.

c. All default passwords are changed to strong personalized passwords and that all services identified by the ~~DMF~~ TLH as unnecessary for the functioning of the system are disabled or removed. Open ports on networks and systems which are not in use are blocked or deactivated and measures are taken to secure them.

d. Adequate capacity to ensure the availability of data is maintained.

e. Integrity checking mechanisms are employed to verify software, firmware, and

[8] Rule 13.3 Client Record Keeping, Rulebook of The Exchange, 2015 (Dealing Members' Rules) states that all instructions given by clients to execute transactions and all other client records in sub-rule (a) above must be kept for at least six (6) years after the rendering of the services concerned;

information integrity.

f. The development and test environment(s) are separate from the production environment.

g. Controls are put in place around the use of devices such as mobile phones, photocopiers, scanners, etc; that can capture and transmit sensitive data, and policies are defined for the connectivity for such devices within their critical IT infrastructure.

4.4 Patch Management

~~DMF~~ TLHs are required to:

a. Document procedures for the identification, categorization and prioritization of software patches and updates in a timely manner.

b. Perform testing of security patches and updates, before their deployment into the production environment to ensure that the application of patches do not adversely impact the systems.

4.5 Maintenance and Repair

~~DMF~~ TLHs shall ensure that:

a. Maintenance and repairs of servers/appliances and information system components are performed in line with ~~DMF~~ TLH's board approved policies and procedures.

b. Maintenance and repair of organizational assets are recorded in a timely manner, with approved and controlled tools.

c. Remote maintenance of organizational assets is approved, recorded, and performed in a manner that prevents unauthorized access in line with the ~~DMF~~ TLH's board approved access control policy.

4.6 Disposal of Data and Storage Devices- Data-Disposal and Data Retention Policy

a. ~~DMF~~ TLHs shall ensure the formulation and implementation of a data-disposal and data retention policy which shall identify the value and lifetime of critical data, and prescribe the process for the disposal of storage media and systems. This lifetime of critical data shall be no less than six (6) years.

b. The data-disposal and data retention policy shall include the removal of critical and sensitive data on all devices and systems employed.

4.7 Vulnerability Assessment and Penetration Testing (VAPT)

~~Dealing Member~~ Trading License Holders shall ensure that:

a. VAPT[9] are conducted on online trading portals twice a year in accordance with The Exchange's Rules on Online Trading Portals[10] and as amended by The Exchange from time to time, and that certified penetration test reports are submitted to The Exchange.

b. Vulnerability scanning and penetration testing are conducted prior to the commissioning of a new system that will be accessible over the internet.

c. Remedial actions are taken immediately to address gaps that may be identified during VAPT.

d. Where an IT Firm is engaged by the ~~DMF~~ TLH to oversee the appropriate management of the ~~DMF~~ TLH's cybersecurity risks, the IT firm shall not carry out VAPT on behalf of the ~~DMF~~ TLH.

5.0 Detection

To facilitate the timely discovery of cybersecurity events, ~~DMF~~ TLHs shall:

a. In a timely manner, establish processes to continuously monitor unauthorised or malicious activities including unauthorised access, duplication, alteration, or transmission of critical data.

b. Establish and manage a standard level of network operations, expected data flows for users and systems, and alert thresholds.

c. Ensure that the physical environment, network systems, information assets and personnel activities are monitored to detect and identify cybersecurity incidences, and to verify the effectiveness of protective measures undertaken.

d. Monitor connections, devices, and software for malicious and/or unauthorized codes.
e. Frequently review and monitor the activities of employees and other users to ensure adherence with the cybersecurity policy and data-disposal & data retention policy.

[9] ~~Dealing Member~~ Trading License Holders shall engage vendors that have been approved VAPT vendors from the Association of Securities Dealing Houses of Nigeria (ASHON) to perform VAPTs.
[10] http://www.nse.com.ng/regulation site/Dealing%20Members%20Rules/Amendments%20to%20Dealing%20Members%20Rules%20(Part%20IX)%20-%20Online%20Trading%20Portal%20Rules%20-%20SEC%20Approved%20August%202019.pdf

f. Implement suitable mechanisms to control the inflow and outflow of network traffic, and monitor capacity utilization of its critical systems and networks that are exposed to the internet, to ensure high resilience, availability and timely detection of attacks on such systems and networks.

g. Ensure that incident data from multiple sources and sensors are aggregated, correlated, and analyzed to understand attack targets and methods.

h. Ensure that information on incident detection is communicated to appropriate parties and that detection processes and procedures are tested and improved regularly to ensure timely detection of incidents/events.

6.0 Response

6.1 The ~~DMF~~ TLH's response plan should define responsibilities and actions to be performed and by whom in the event of cyber-breaches or business disruptions.

6.2 ~~DMF~~ TLHs shall ensure that:

a. Board approved response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

b. Alerts generated from monitoring and detection systems are immediately investigated to determine activities necessary to isolate, diagnose and mitigate the effects of the cyber-attack or breach.

c. Pre-defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are included in ~~DMF~~ TLH s' business continuity and disaster recovery plans for timely restoration of systems in the event of cyber-breaches or business disruptions.

d. Business continuity/disaster recovery tests are conducted at least once a year in order to test the adequacy and effectiveness of their Business Recovery Plan.

7.0 Recovery

7.1 Recovery planning and processes shall be continuously improved by ensuring that any incident, loss, or destruction of data or systems are analyzed to ensure that the impact is fully understood, and that lessons learned from such incidents are subsequently incorporated to strengthen the security mechanism and improve recovery planning and processes.

7.2 ~~DMF~~ TLHs shall ensure that:

a. Recovery processes and procedures are executed and maintained to ensure timely restoration of systems, processes or assets affected by cybersecurity events.

b. Restoration activities are coordinated with internal and external parties - such as service providers, customers/clients and vendors etc.; such that communications with clients are managed effectively.

8.0 Training and Education

8.1 ~~DMF~~ TLHs shall ensure that there are continuous information security awareness and training for its staff, and by extension all outsourced staff, vendors, clients and other stakeholders who may be granted access to ~~DMF~~ TLHs' information systems. This includes training and awareness on password security, secured remote connections, phishing and other related cyber risk awareness training.

8.2 At a minimum, training and awareness programs shall include: password handling, identification of secure websites, risks of using external storage drives, safe internet behaviour, conducting business over unknown public internet connections, system idling protocols, and use of personal mobile devices for official business. Such programs shall require post training assessments and participation in all drills/penetration testing, which shall be evidenced by documentation.

8.3 In the event of an inquiry/examination by The Exchange, evidence of participation in Training and awareness programs shall be provided to facilitate an assessment of ~~DMF~~ TLHs' compliance with this requirement.

8.4 Training and awareness programs shall be reviewed and updated regularly by the ~~DMF~~ TLHs to ensure they remain relevant.

9.0 Sanctions

Non-compliance with the provisions of these Rules shall attract appropriate sanctions as may be determined by The Rulebook of The Nigerian Stock Exchange.