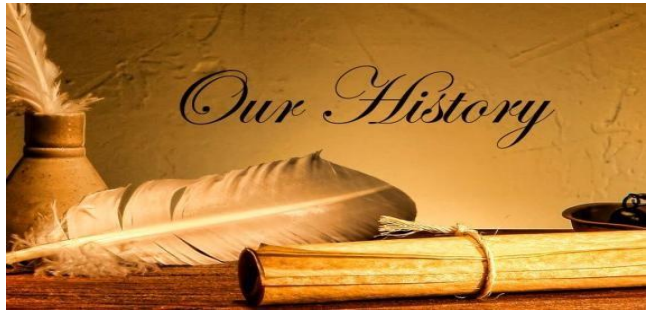
NIGERIAN STOCKBROKERS LIMITED

(Trading Licence Holder)

INFORMATION TECHNOLOGY POLICY

Table of Contents



Incorporation and History

Nigerian Stockbrokers Limited ('NSL'/ the company) was incorporated as the first stockbroking firm in Nigeria under the Companies Ordinance Cap 38 on 26th September 1960. Prior to the implementation of the Nigerian Enterprise Promotion Act 1972 ('Indigenisation exercise') NSL was wholly owned and managed by Financial Holdings Nigeria Limited ('FHNL'). Following the Indigenisation exercise, the interest of FHNL was transferred to some Nigerian citizens and association. NSL is, therefore, a wholly owned Nigeria company.

The Company obtained a Broker/Dealer license from the Securities and Exchange Commission ("SEC") in 1995 and subsequently became an Authorized Dealer of the Nigerian Stock Exchange ("NSE"). NSL had a composite licence for its business operations from the Securities & Exchange Commission (SEC).

Nigerian Stockbrokers Limited (NSL) is a first class Investment banking Group. The authorized and paid-up share capitals steadily increased over the years to meet both business and regulatory requirements. Since the Management Buy –Out in 2016, NSL has been modelled after major international investment banking institutions. The Company is ably managed by a team of time-tested and visionary professionals. It has since grown steadily in the various aspect of capital market operation and has NSL Capital Partners Limited as a subsidiary with operations in the Investment Banking and Capital Advisory space of the market.

NSL's Corporate Head Office is located at Knight Frank Building, 6th floor, 24 Campbell Street, in the highbrow of the Central Business District of Lagos Island, Lagos State, which provides a convenient environment for clients away from the busy city centre; thus facilitating personalized and efficient service delivery to its numerous corporate and individual clients.

SERVICE MANAGEMENT FRAMEWORK

Service Management is a required component to achieving the strategy of the IT group. Service management describes strategy with which IT Services will be delivered to the business in a way that consistently provides value to internal customers. A service management plan helps us achieve the following:

- Reduction of the service delivery costs
- Understand and define the business impact of all IT Services
- Definition of Service components and configuration items to enable capacity building and forecasting and ensure service level agreements are met
- Improved internal and external customer satisfaction levels

Service Management Strategy

- Document and deliver on all service availability agreements for all IT services
- Develop capacity and flexibility on an enterprise scale to ensure reduced time to market for all initiatives within the business
- Measure and monitor all services to ascertain business value and identify opportunities for improvement
- Define and measure performance indices for the IT group
- Drive knowledge sharing to ensure we maintain a workforce which is in tune with the corporate climate and acutely aware of their role in the success of the organization as a whole

Service Portfolio Management

Service portfolio management is the management of all services currently being delivered and controlling the process by which new services and designed. Service portfolio management classes IT services into three buckets; Services in the Pipeline, Services currently being offered and retired services. Pipeline services are services which have been envisioned and are awaiting design and implementation.

Services currently being offered are services which are documented in the IT Service Catalog as services which can be subscribed.

Retired services are services which have lost their relevance and are no longer required. These services are then retired and taken off the Service Catalog.

Service development lifecycle

The IT service lifecycle describes the life of an IT service, from planning and optimizing the IT service to align with the business strategy, through the design and delivery of the IT service, to its ongoing operation and support.

For all services, these phases serve as a check list to ensure all considerations have been evaluated. The rigor with which they will be applied is determined by the scope and impact of each service.

The service development lifecycle adopted is based on the Microsoft Operations Framework which has four basic phases:

Plan Phase:

- Business/IT Alignment: Review business value of the proposed service to ensure alignment with the IT Strategy and the overall corporate strategy.
- Performance metrics: Performance metrics from the customer‘s perspective to understand what would constitute value from the view of the customer.
- Procedures and Policies: Review the impact of this service on existing business processes and identify gaps which may require new policy definitions Fiscal Management: Evaluate effort required to develop service. Review budgeting constraints alongside fiscal benefits.

Deliver Phase:

- Visioning: Document the end state which would be achieved by deploying the service. Detail a migration plan and guidelines for moving from current state to proposed end state
- Plan Execution: Evaluate available options and technologies. Evaluate available resources if local development will be done. Document functional specifications and project plan
- Build: Develop or acquire required applications, identify release dependencies. Release Management: Review service to ensure —fit-for-purpose‖ and —fit-for use‖ from the perspective of the customer. Prepare production environment and perform controlled pilot
- Deploy: Deploy service to production environment

Operate Phase:

Identify operational work requirements i.e. dependencies that ensure the service can be used by the customers for which it has been designed Service Delivery Management: Hand over service to service delivery manager. Manage customer experience, ensure SLAs are met, incident and problem management Service monitoring and measurement: Monitor overall health of the service and all its

dependencies. Manage incidents and ensure continuous improvement

Manage Phase:

- The manage layer continuous for the entire lifecycle and happens in parallel for all lifecycle phases
- Risk management: continuously manage all potential risk factors which may impact the service or which may be enabled by service deployment
  Change control: Ensure all changes are done using formal change control process

Service Management Policies

Effective service management is dependent on ensuring that defined processes are followed and operations happen in a controlled manner.

Some policies which are pertinent to a successful service delivery strategy include:

- Change management policy
- Project documentation standards
- Technology acceptable use policy
- Password policy
- Internet use policy
- Backup and Retention Policy
- IT Device Naming Convention
- IT Portfolio Management Framework
- IT Security Policy
- Associated Documents
- IT Service Catalog
- IT service dependency maps

INCIDENT MANAGEMENT FRAMEWORK

An incident is an unexpected service disruption which may or may not be anticipated. As is expected with any technology service, disruptions occur making it critical as part of the effective service delivery process to document a process for handling all incidents, communicating to affected users and keeping customers in the update loop until resolution. Incident Management

All IT related incidents and service requests within NIGERIAN STOCKBROKERS LIMITED are handled centrally by the IT Service Desk using the following process:

Incident Management Process

Incident Classification

Incidents are categorized largely based on scope of impact and effect of business continuity. The incident categories are:

Incident Management Process

Priority 1 This refers to incidents affecting Line of Business Enterprise Wide Categorize Incident Logged applications and impact directly on the business in terms of revenue and customer service delivery

Priority 2 This refers to incidents that affect a smaller group of Limited number people like a unit, department or branch and for which a of users work around can be provided Assign to Service

Priority 3 This refers to an incident which has no immediate impact Very limited Desk Support for Known Problem? N First Level Support on customer service delivery number of users

The categorization of incidents is done using the impact – urgency matrix as shown below: Y

High Low

Classify as problem and escalate to High HH – Priority 1

LH – Priority 2

Third Level Escalate to Second Resolved within Refer user

N Level Support SLA? Knowledge Base

Low HL – Priority 2 LL – Priority 3

Technology Acceptable Use Policy

To consistently provide and meet all expectations from the business technology tools which are used to provide or deliver service, there is a need for a policy to define what constitutes acceptable use of the company‘s assets which are in the care of the company‘s staff. This document serves to be the first point of exercising control over all technology related tools and devices provided by the IT group.

Scope

Policies defined in this document apply to all technology tools and related services provided or used by the IT group and the company as a whole.

Policy Statement

Computer and technology tools provided by the IT group are to be used in carrying out the company’s business functions and, as such are intended for job-related purposes only. All users irrespective of grade/level are expected to make a formal request to the IT department before being granted or assigned any tool or access level for use. A user is expected to sign an acknowledgement form on receiving access to any of the system in use within.

Information Asset Classification

For the purpose of this policy, information assets are classified into 2 broad categories:

Devices

This refers to all tools and hardware which are used within the company's network or can be used to reach the company's network from outside the company's premises. Devices covered under this include:

- Smart Phones
- BlackBerrys
- Laptops
- Desktops

For the purpose of this policy, devices covered are not restricted to devices which are provided by the company or not.

Device Management Standards

All devices used within or used to access the NIGERIAN STOCKBROKERS LIMITED network are subject to Global policy rules without prior notification to the device owner

- All devices used within or the NIGERIAN STOCKBROKERS LIMITED network must conform to the security and configuration standards as put forward by the Network and Communications team of the IT group
- Any devices which do not conform to the standards of the IT group can be denied access to the network without prior notification to the device owner
- All devices provided by the company remain the property of the company and can be retrieved and replaced when required.
- The IT group reserves the right to monitor activity and intercept network traffic on any device used to access the NIGERIAN STOCKBROKERS LIMITED network
- The IT group reserves the right to update virus definitions, operating systems and other system parameters without prior notification. These updates should not be removed on uninstalled by users as doing do may lead to denial of assess.
- The IT group reserves the right to back up all information stored on any device within the network to a central location. This included personal information stored on the devices.
- All devices removed from any NIGERIAN STOCKBROKERS LIMITED premises by an individual must be documented, including the model, manufacturer and serial numbers on an IT supplied form.
- When an employee resigns his/her appointment with NIGERIAN STOCKBROKERS LIMITED or is dismissed, he or she must return all devices allocated prior to the last day of employment

Media

Company network.

For the purpose of this policy, media refers to:

- The Corporate Intranet
- The Internet
- The Corporate Website
- All messaging and collaboration platforms
- All applications used within the company including the Core Company System
- All documents
- The Corporate Network

Details

- All information provided or accessed via any media except when otherwise stated is proprietary to NIGERIAN STOCKBROKERS LIMITED and can only be used for the business of NIGERIAN STOCKBROKERS LIMITED
- The IT The group reserves the right to monitor communication and data at any time, with or without notice, to ensure that company property is being used only for business purposes.
- The IT group reserves the right to deny access over any media or to any information available on any of these platforms when deemed necessary
- The company reserves the right to disclose the contents of messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of Human Capital Management (HCM), unless otherwise stated
- Employees are not authorized to retrieve or read e-mail messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so
- Emails with attachments which are deemed to be potential threats to the network will be prevented from delivery without prior notification to the sender. Attachment extensions which fall under this category are —.wmv, —.pps, —.mpeg, —.mp3, —.wav. wma, —.avi, —.mp4, —.mps
- The messaging system is not to be used to solicit for commercial ventures, religious or political causes, or other non-job-related solicitations.
- The messaging system is not to be used to create any offensive or disruptive messages
- Only legally licensed software will be installed on computers. Users are expected to request for any software required to carry out their duties through the IT Service Desk

- The IT group will configure all workstations with virus protection software, which should not be removed or disabled
- The IT group will implement and maintain procedures to provide adequate protection from intrusion into organization's network from external sources
- All access rights in form of logon profiles will be disabled when staff have resigned, dismissed or are otherwise unavailable officially (study leaves and vacation inclusive)
- The Internet is to be used for business purposes only. Employees with Internet access are expressly prohibited from accessing, viewing, downloading, or printing pornographic or other sexually explicit materials
- Internet Access levels are defined in the Internet Use Policy and apply to all staff
- Employees are expected to use the standard software provided by IT, or request applications they need in the course of their work through the Service Desk.
- Employees are not permitted to download applications, demos or upgrades. Employees will use the standard e-mail system provided by the group for official e-mail communications, and should not install their own e-mail clients.
- Use of instant messaging programs, such as ICQ, AOL Instant Messenger, Yahoo Messenger, etc., is prohibited unless otherwise approved by management or the IT department.
- IT will monitor network security on a regular basis. All information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected

Violations

Failure to comply with all components of the technology resource usage policy may result in disciplinary action. Any employee who does not understand any part of the policy is responsible for obtaining clarification from his or her manager or the IT Service Desk.

PASSWORD POLICY

Passwords are an important aspect of enterprise security. They are the front line of protection for the enterprise network. A poorly chosen password may compromise an entire corporate network. As such, all employees (including Contractors and vendors with access to system resources are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation and maintenance of secure passwords, the protection of those passwords and the frequency of change.

Scope

The scope of this policy covers all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides within NIGERIAN STOCKBROKERS LIMITED, has access to the organization‘s network, or stores any public or non-public organizational information.

Password Standards

Passwords should neither be too short nor too long. The length of the password will, at all times, comply with the laid down password creation rules. A passphrase can be used when available at application level.

- All user-level and system-level passwords must conform to the password complexity guidelines.
- All applications should enforce regular password changes every 30 days and not permit previous password(s) to be used for at least 3 months after being changed.
- Passwords must not be inserted into email messages or other forms of electronic communication
- Passwords are case sensitive and must be used in the exact case they were created

Password Complexity Guidelines

- All passwords must be at least six characters long
- All passwords must be alphanumeric i.e. contain letters and numbers
- All passwords should have a combination of upper and lower case characters (Capital and Small letters)
- All passwords must include special characters such as (!, *, #, @, &, %, $
- Passwords or parts of the password cannot be re-used when creating new passwords
- Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet‘s name etc.)

Password Protection

- Employees, Vendors and Contractors must not share passwords with anyone. All passwords are to be treated as sensitive, confidential information
- Employees, Vendors and Contractors must not write passwords down and store them anywhere in the office. Passwords are not to be stored in a file on any computer system without encryption.
- If an account or password is suspected to have been compromised, report the incident to security administrator and change all passwords
- Password cracking may be performed on a periodic or random basis by the security administrator. If a

password is guessed or cracked during one of these scans, the user will be required to change.

- Application developers must ensure their programs contain the following security precautions:
- Application should support authentication of individual users, not groups.
- Application should not store passwords in clear text or in any easily reversible form.
- Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

If for unavoidable reasons (for example during remote support or when working with vendors remotely) passwords are shared, such passwords must be changed in the shortest possible time to avoid misuse. In addition, all such incidents must be documented and a self-audit carried out immediately after the change to ensure the password has been changed.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

All vendors and contractors must sign a Non-Disclosure agreement prior to being given access to the NIGERIAN STOCKBROKERS LIMITED network to treat all information given to them confidentially.

Equipment Maintenance:

All IT equipment will be maintained to ensure maximum up-time and useful life and minimal unexpected maintenance.

Servers:

All Servers are scheduled to have maintenance performed weekly and monthly by IT staff via a prescribed list of tasks.

PCs'

Each server and PC desktop is automatically password locked (3 mins) when not in use, requiring a domain username and password to access the servers.

All PC's are required to have Virus prevention software, Anti-Spyware software as well as any additional safety measures based on individual PC needs. Updating of virus/spyware definitions and database engines shall be automatic and monitored for performance.

Monthly PC maintenance shall be provided to all PC's ensuring; all automated services are working properly, all software and hardware updates are current, no excessive local file storage, optimal system speed, etc

Other Equipment:

All other equipment, i.e., generators, copy machines, etc. will be maintained based on the manufacturer's recommendations and any service agreements.

Security:

Nigerian Stockbrokers Limited faces numerous challenges securing its various information systems including its data.

- **Identify the need to protect information:** Nigerian Stockbrokers Limited sustains an ever growing compilation of electronic data from financial information to operational data. Accessing and storing this information is critical to the viability of the organization.

- **Define authorization levels for administrators and users:** Authorization for all data has been analyzed and is tested to ensure those individuals needing the information have access and those who do not, are blocked
- **Define and Detect Security Threats Internally and Externally:** As the number of types of security threats increase, staff incorporates new measures to detect all known threats without significantly affecting the information flow across the network.
- **Implement a comprehensive monitoring policy:** On-going security tests are performed to determine if initial security settings are correct as well as to detect any inappropriate changes to security. Measures are added as needed to ensure a comprehensive detection process is utilized.
- **Define an IT Policy to handle Security Violations:** Nigerian Stockbrokers Limited has created both an in-house and web policy to determine parameters for what staff and web users should and should not be doing. If they cross that line, quick measures will be taken to ensure the overall Safety and Security is maintained at Sterling.
- **Correlate this policy with detected security events:** Specific security violations are specified when applicable.
- **Create and Maintain a Disaster Recovery Plan:** Nigeria Stockbrokers Limited's Disaster Recovery Plan includes Information Technology as a critical piece to successfully recovering from a disaster. This plan is updated periodically as changes are made.

Active Directory:

We utilize an AD Domain Controller server to provide redundant Active Directory/Domain services such as DNS, WINS, DHCP, Print Servers, Domain Controllers, File Servers, etc.

When assigning data access rights to users, group objects are used versus user names to decrease long term cluttered rights assignments and to help with ensuring outgoing employees do not have any access they should not, due to inadvertent additional user right.

The Systems Administrator periodically peruses through the various sections of AD and cleans up stale resources, searches for and eliminates duplicated entries, breaks out complex GPO's into more manageable objects, etc.

Users:

- Domain Administrator Account renamed and relabelled.
- Domain Admin Account password changed periodically.
- Guest Account renamed and disabled.
- Contractors requiring access to Network are given username/password which expires.
- Security of files and folders is maintained using AD Groups, eliminating difficult-to-manage stray user names.
- Weekly listing of folder permissions is provided to the Quality Assurance Office for review accuracy and indication of more effective changes to be made.

This Manual has been Reviewed and Approved by the Board of Directors of Nigerian Stockbrokers Limited at its meeting held

This 28th Day of March, 2026

…….. ……..

Company Secretary Director