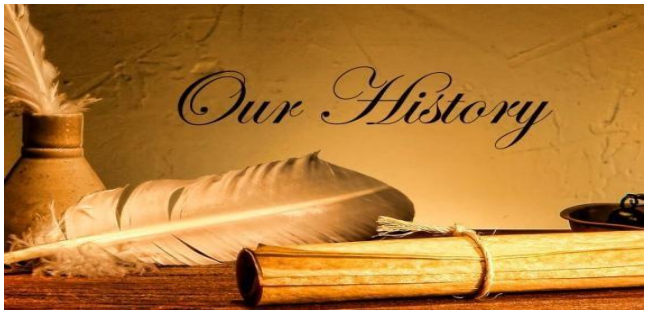
NIGERIAN STOCKBROKERS LIMITED
(Trading Licence Holder)

INFORMATION SECURITY, BACKUP, BUSINESS CONTINUITY & DISASTER RECOVERY POLICY

TABLE OF CONTENT:



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.

VISION & MISSION STATEMENT

To be a dynamic Stockbroking firm. Providing the best investment advice and qualitative services in the most effective and efficient manner using up to date market information, technology and Committed staff to select clientele.

IT SECURITY

Information security aims to protect information and communication assets, and ensure business continuity by preventing and minimizing the impact of information security incidents. Information security (IS) provides the trusted environment that the company needs to be confident in adopting efficient new ways of doing business. There are three basic elements to information security that must be maintained at all times to protect against loss, damage and unauthorized disclosure of information:

- **Confidentiality**: protecting sensitive information from unauthorized disclosure or interception.
- **Integrity**: safeguarding the accuracy and completeness of information and computer software.
- **Authenticity**: verifying an identity claimed by or for a system entity to forestall unauthorized access and alterations to system, data and device configuration.

Scope

Information Security is of importance to all employees of Nigerian Stockbrokers Limited (NSL/the Company), including temporary Staff and contractor personnel. Conformance to this IS Management Framework is therefore required from the moment an employee joins NSL until the moment he/she leaves.

The scope of this information security policy includes NIGERIAN STOCKBROKERS LIMITED computer and telecommunications systems and the employees, contractors, temporary personnel and other personnel of the company who use and administer such systems. This IT Security policy applies to every division or subsidiary of NIGERIAN STOCKBROKERS LIMITED established by the laws of Nigeria for the exercise of any function of the Group except for those specifically exempted.

It relates to all types of information in any format (i.e. paper, electronic, audio, video, etc.) including sample or draft (stored, in processing or transit). It also relates to all information management and communication assets. Background

Security risks associated with information technology are increasing in both number and variety. Information technology network infrastructures are increasingly more complex to implement and administer. The advent of hacking tools and persons willing to distribute viruses and malicious code has increased the risks to IT organizations and the assets they are charged to safeguard.

Company-critical functions supported by IT systems continue to expand. Although some data and systems may not be classified as mission critical, they nevertheless represent a significant investment in resources, contain sensitive data, and are efficient methods of providing a wide range of financial services. Coupled with overall system integration and interconnectivity, companying systems and networks are increasingly at risk to intrusions, misuse of data, and other attacks from both internal and external sources. The Nigerian Stockbrokers Limited IS Policy, —Information Security Framework is intended as a tool to mitigate increased risks.

A successful security framework is reliant upon strong leadership support and a comprehensive body of effective and efficient information technology security policies and procedures that serve to:

- Promote public trust
- Ensure continuity of the company's financial services
- Comply with legal requirements
- Recognize risks and **threats**
- Protect **system assets**

Information Security Principles

The following are the key information security principles which are fully in line with the ISO/IEC 17799:2005

- Information Assets must be protected against loss or damage. Offices, facilities and IT services must be protected against unauthorized access.
- Sensitive information and essential IT services should be safeguarded from security threats.
- Business will be able to continue following (IT) failures or disasters affecting business locations.
- Information should be shared safely, for the benefit of the businesses, as widely as possible across Nigerian Stockbrokers Limited and its subsidiaries.

Responsibilities

All NIGERIAN STOCKBROKERS LIMITED employees are responsible for adhering to this policy.

Employees

All employees (including Contract staff) should safeguard the information that they create, receive or control, as well as the IT services that they use or provide.

They are required to:

- Make themselves familiar and comply with the NIGERIAN STOCKBROKERS LIMITED information Security policy, standards and any relevant legislative and contractual Information Security requirements
- Attend prescribed Information Security awareness trainings
- Report any actual or potential Information Security incidents or weaknesses
- Follow local procedures for protection against viruses
- Observe all relevant user-oriented guidelines, including password management, information classification and access to restricted areas
- Ensure that equipment and media have appropriate security protection
- Operate the clear desk policy
- Ensure Company IT facilities are only used for authorized business purposes
- Comply with legislative and contractual requirements by only using approved and licensed software.

Information Security Officer

The role of the Information Security Officer (ISO) is to implement the NSL's security policies and practices, identify additional security measures where necessary, promote and co - ordinate these activities throughout the group. The Information Security & Assurance Officer will essentially play the role and perform the responsibilities of Focal Point when it comes to issues relating to information security planning and management.

In addition, The ISO will:

- Establish and maintain a business-aligned corporate framework for Information Security management
- Direct, support and review the execution of Information Security activities
- Develop short-term information security strategy
- Establish and maintain appropriate Information Security management forum
- Define and agree corporate Information Security responsibilities
- Contribute to identification of security concerns and implementation of countermeasure in all IT related projects
- Identify and assess sources of threat to the security of Company information assets
- Co-ordinate rollout and compliance with Group Information Security policies and practice, company wide
- Provide security advice and support to all NIGERIAN STOCKBROKERS LIMITED employees, including vendors and contractors.
- Ensure that appropriate documentation of policies, standards and guidelines are published
- Initiate and direct Information Security appraisal on an on-going basis
- Monitor Information Security incidents affecting services
- Develop and monitor progress against a business-aligned Information Security plan
- Coordinate a program of Information Security education and awareness
- Contribute to reviews of new security technology

Group Head, IT & Operations is responsible for enforcing this policy.

IT Security Policy

Policy Statement

NIGERIAN STOCKBROKERS LIMITED employees, contractors and vendors shall exercise due diligence to ensure that computer and telecommunications systems and services that conduct or support company business are secure, and that the information contained within those systems and services is protected from unauthorized disclosure, modification or destruction, whether accidental or intentional.

The information security advisory team, as part of an overall security management strategy, shall develop internal information security policies. In addition, the company policies and procedures shall ensure compliance with all federal and State security-related regulations that apply to the company's mission and services. The company shall ensure that employees, vendors and contractors are aware of their specific information security responsibilities in the use of the company information systems and the handling of information.

Minimum Security Requirements

The following minimum-security requirements provide the foundation for IT security policy development and are described in more detail in this policy.

- Risk Management: NIGERIAN STOCKBROKERS LIMITED shall apply risk management techniques to balance the need for security measures
- Confidentiality, Integrity and Availability: NIGERIAN STOCKBROKERS LIMITED shall ensure that security policies, plans and procedures address the basic security elements of confidentiality, integrity and availability

- Protect, Detect and Respond: NIGERIAN STOCKBROKERS LIMITED security plans and policies shall include methods to protect against, detect, and respond to threats and vulnerabilities to information and systems.
- Identification and Authentication: NIGERIAN STOCKBROKERS LIMITED shall implement an identification and authentication process for information systems and services
- Access Control and Authorization: NIGERIAN STOCKBROKERS LIMITED shall implement access control and authorization policies, plans and procedures as required to protect system assets and other information resources maintained by the company
- Security Audit Logging: NIGERIAN STOCKBROKERS LIMITED shall implement a security audit logging capability on information systems, including computers and network devices
- Security Management and Administration: NIGERIAN STOCKBROKERS LIMITED shall implement a security management and administration program.

Risk Management

NIGERIAN STOCKBROKERS LIMITED shall adopt a risk management methodology that incorporates the following risk management processes:

- Risk Assessment: Positions the company to determine effectively the extent of potential threats and the associated risk. The goal of conducting a risk assessment is to identify financial services / company-specific controls that are appropriate for reducing or eliminating risk
- Risk Mitigation: Addresses the prioritization, evaluation and implementation of strategically selected controls. The goal of risk mitigation is to select and implement controls that reduce risk to an acceptable level; and
- Evaluation and Assessment: Is a process comprised of activities that recognize and respond to new and changing risks, measure the effectiveness of implemented controls, and modify controls to reflect changes in the three aspects of risk management: operational, technical and managerial. The goal of evaluation and assessment is to maintain a successful and effective risk management program that continuously evolves and responds to changing threats and opportunities. Risk management offers a practical approach to balancing security with operational requirements and cost. The definition of acceptable risk and the approach to managing risk can vary for each agency. Risk management is a trade-off in which a certain amount of residual risk is accepted as a balance to the costs of incremental countermeasures. The likelihood that adverse events will occur is determined by analyzing possible threats in conjunction with vulnerabilities and potential business impact. The formula that follows is commonly applied by the information security community to define and measure such risks as a part of risk management. The formula further expresses the relationship of risk exposure factors to counterbalancing security strategies in defining the level of risk:

Risk = Impact x Threats x Vulnerabilities Countermeasures

Risk factors are defined for each system being measured and receive relative ratings of high (H), medium (M), or low (L). As an example, risk factor ratings for a hypothetical company Web server that is linked to customer records might be as follows:

- Impact – The impact of a successful attack to obtain or change a customer's account details might be rated as —high.
- Threat – The likelihood of an attack might be rated as —medium.
- Vulnerability – The system in this example has no protective measures for the server and therefore vulnerability would be rated as —high.
- Countermeasures – Alternative measures are robust and therefore would be rated as high.

In this hypothetical example, the robustness of the countermeasures may reduce or mitigate the overall risk, resulting in an acceptable level of risk. The NIGERIAN STOCKBROKERS LIMITED risk management practices shall include the elements described in sections 2.3.2.2 through 2.3.2.4 below.

Risk Assessment

All departments shall periodically conduct a risk assessment of system assets to address changing threats and organizational priorities. Risk assessments shall:

- Identify IT systems, resources and information that constitute each system and prioritize the relative importance of the system assets
- Identify and document potential threat-sources
- Identify and document system vulnerabilities that could be exploited
- Analyze security controls that have been implemented or are planned for implementation that minimize or eliminate the likelihood of a compromise occurring
- Determine the likelihood of potential vulnerabilities being exercised by a threat-source.
- Determine the impact associated with the compromise of the company's system assets
- Determine the level of risk using a rating methodology such as high–medium–low

- Identify technical, operational and management controls that can mitigate or eliminate the identified risks; and
- Document risk assessment results and control recommendations.

Risk Mitigation

NIGERIAN STOCKBROKERS LIMITED shall prioritize the implementation of mitigation actions based on the results of the risk assessment. Risks may be eliminated, mitigated, shared with one or more third parties, or accepted. If certain risks are to be eliminated or mitigated the agency shall:

- Evaluate and compare the security countermeasures available and the resources required to implement them, with the resources required to replace the system assets.
- Determine which countermeasures are reasonable to employ.
- Establish guidelines for implementing management, operational and technical security controls commensurate with the established risk to system assets.

Evaluation and Assessment

The information security risk management team shall periodically evaluate security controls to determine their ongoing appropriateness and effectiveness for current and anticipated risks and update controls based upon the findings.

The Information Security & Risk Management teams shall ensure that internal security policies, plans and procedures address the fundamental security elements of confidentiality, integrity and availability.

Confidentiality standards

Businesses and employees expect that sensitive information about them will be shared only with those who need access, that the information will not be altered either by accident or malicious intent, and that it will be available when needed. To this end, the Systems or Database Administrator shall:

- Provide information and services only to those authorized.
- Protect information so that it is not altered maliciously or accidentally.
- Ensure that information and services are provided in conjunction and accordance with the company's business continuity policy

Protect, Detect and Respond

Policy Statement - The Company's IT security plans and policies shall include methods to protect against, detect and respond to threats and vulnerabilities.

Standards

At a minimum, the company shall:

- Determine how much protection is needed and for how long, per the results of the risk assessment and then develop policies and procedures accordingly.
- Develop a methodology to detect when system assets are safe and when they are threatened. The methodology needs to include auditing and recording the status of all protected system assets at intervals appropriate to the risk as defined in the assessment.
- Develop the company's security incident reporting policy describing how to respond to security incidents that addresses who, what, when, where and how?
- Develop a policy identifying the types of services and protocols permitted by the network systems, both within the network and crossing the network boundary. The fundamental policy strategy for services and protocols external to the network must be to —deny everything‖ and allow only specific services and protocols on a case-by-case basis. NIGERIAN STOCKBROKERS LIMITED shall employ security precautions for the management of such services pursuant to NIGERIAN STOCKBROKERS LIMITEDIT Policy - ITPOL.14, —TCP-IP Implementation Standards.

Identification and Authentication

Policy Statement - NIGERIAN STOCKBROKERS LIMITED shall implement an Identification and Authentication (I&A) process for information systems and services that require controlled access. The identification process shall require the user to present a valid identity using a recognizable method. 6.6.2 Identification and Authentication Standards. The most common form of identification is a user ID. The authentication process shall require the user to present verification of identity in a recognizable format. The most common form of authentication is a password. For I&A, NIGERIAN STOCKBROKERS LIMITED shall meet the requirements listed below:

- System **users** shall have unique and individual user IDs
- User identities shall be validated before issuing user IDs and other credentials. Procedures shall be established for maintaining and managing system user IDs, including procedures for establishing new user accounts, validating existing user accounts, and terminating former user accounts. Inactive

user IDs shall be deactivated after a period of no activity, not to exceed six months

- All user credentials shall be protected from unauthorized access and alteration
- A security credentials distribution process shall be developed that ensures the confidentiality, integrity and availability of security credentials such as passwords, PINs, **biometrics,** tokens and certificates. Password and PIN processes shall fulfill the requirements of NIGERIAN STOCKBROKERS LIMITEDIT Password Policy.
- If a user is locked out of a system due to a forgotten password, data entry mistake while entering a password, or any other legitimate error, the company's security procedures shall verify valid identification and authentication before permitting access.
- If a NIGERIAN STOCKBROKERS LIMITED network user is using, sending or receiving legally binding electronic records or signatures, the I&A process shall comply with the NIGERIAN STOCKBROKERS LIMITED Information Sensitivity Policy.
- An authentication process commensurate with the risk assessment of the system assets shall be established. Robust methods of authentication, such as **two-factor authentication** or **digital certificates,** shall be employed to limit access to systems that contain data requiring more secure access or information whose disclosure would cause serious disruption or harm.

Policy Statement

The company shall implement access control and authorization policies, procedures and plans to protect NIGERIAN STOCKBROKERS LIMITED information resources.

Access Control Standards

Access control addresses the securing of systems, both the hardware components and the software components. Authorization addresses the management of permissions to access the various system components, including processes for approving access and restricting access. Restricting access can apply to both invalid users and valid users with limited privileges. To this end, the company shall:

- Secure system assets from physical access by unauthorized persons at all times. At a minimum, system assets shall be in the control of authorized personnel or protected by a locking mechanism.
- Manage systems with appropriate access control processes and well-formulated **access control lists.**
- Use the **least-privilege** method for granting access to system assets.
- Subject all personnel with access to system assets to a **vetting process** that is commensurate with the system assets risk assessment
- Ensure that systems can detect and deny unauthorized transaction attempts by any user. Unauthorized attempts shall be logged in accordance with the security audit logging requirements
- Implement any restrictions to accessing systems outside of normal working hours.
- Ensure that the access control methodology can disable user privileges to those who no longer require access.

Security Audit Logging

Policy Statement - NIGERIAN STOCKBROKERS LIMITED shall implement security audit logging on information systems such as computers, network devices, **routers, firewalls,** and applications. Audit logging shall be commensurate with the company's risk assessment findings

The purpose of audit logging is to maintain a consistent and reliable record of system activity. When properly implemented, audit logging can serve as a preventive measure as well as a forensic aid. A comprehensive record of ―who-did-what-when‖ can discourage asset abuse or be a vital form of evidence to prove culpability or prosecute a perpetrator. The company shall:

- Enable security audit features for system assets and configure them to be sufficient to track attempted security breaches. Company shall ensure that their audit strategy captures the information necessary to identify who is accessing NIGERIAN STOCKBROKERS LIMITED system assets, access attempts and failures, and violations of security policy. Appropriate processes shall be put in place to review and analyze the logs commensurate with the agency's risk assessment. Audit logs shall be protected from tampering and available for review.
- Ensure the confidentiality and security of audit information.
- Ensure a separation of duties, where possible, between personnel administering access control functions and those administering security audit logging functions. If these functions cannot be separated, company shall document the reasons and develop a process to address conflict of interest concerns.
- Ensure that audit logs capture information sufficient to satisfy an inquiry to determine timing, events, impact and ownership of both normal system activity and violations of policy, whether security-related or agency business-related. Based upon a deliberate assessment of the organization, application, information and risk, determine an appropriate data collection scheme and retention

schedule for audit logs sufficient to associate specific users with events that breach protocol. If logs are subject to an investigation, they shall be preserved as long as needed.

Procedure 11: User Password Management
Applications often provide own authentication mechanism via the use of username and password combination rather than leverage the OS authentication. Where a separate mechanism is implemented by an application, the following procedure must be adhered to:

- Each user must have a unique user name
- Initial Passwords must be communicated to the user securely
- All passwords for system level accounts, application administrative accounts, system administrator accounts, and database administrator accounts must have the following characteristics:
- Must be changed at least once every 30 days.
- Initial password must be changed by logging into the system within 10 days of issue.
- End user passwords must be changed at least every 30 days
- Users should be advised to change initial password at first use. Where possible, applications must be configured to force password change upon first login
- Passwords must not contain common words or words found in any dictionary.
- Keyboard patterns cannot be used, e.g. qwerty
- Passwords must be changed immediately if they have been given to someone else.
- Passwords must have 6 or greater characters
- Must contain a mixture of alpha and numeric characters, as well as special characters
- The password cannot contain the user's login name
- Passwords cannot be reused until after six (6) passwords.
- Passwords must be changed as soon as possible after a compromise and within one business day.
- User can change his/her password anytime with the system. For the password protection standard and other rules relating to password security management, refer to the NIGERIAN STOCKBROKERS LIMITED IT Password Policy.

Computer Malware
Policy Statement - NIGERIAN STOCKBROKERS LIMITED management and employees, third party persons and temporary staff shall protect information system assets from infections by malicious software, or malware.
As a general rule the following would apply:

- IT Support staff shall install firewalls on all personal computers (workstations) and on all servers.
- IT Support staff shall ensure that operating systems, web browsers, e-mail programs, and related software are configured for optimum security
- IT Support staff shall install an anti-virus program on every PC and all anti-virus software shall be automatically updated through the use of a subscription service (updates should be automatically logged by the software).
- Additional anti-malware programs should be installed on all PC's and servers to protect against nuisances such as spyware and adware, which are potential malware vectors.
- As vendors learn of vulnerabilities (bugs) in their software and repair them, many vendors offer subscription services, through which the IT Group may be notified of security threats and related issues and obtain software patches.
- IT Group should subscribe to one or more notification services, in order to maintain its awareness of threats and to ensure all software is updated in a timely fashion.
- IT Support staff shall evaluate all software patches (for operating systems, browsers, email, programs, applications, etc.) for relevance and criticality. If the patch is determined to be relevant (for example, an operating system security patch has more relevance – and is certainly more critical - than a foreign-language update of an application), IT Support staff shall install the patch in a test environment and verify its effectiveness and compatibility with existing software before installing it in the production environment. Such updates shall be logged by IT Support staff, if the software being patched does not automatically log activity.
- All anti-malware protections shall be configured so as to prevent their being disabled by users. Only IT Support staff, the IT Security Manager, and members of the IT Security staff shall be allowed to temporarily disable anti-malware measures (for example, disabling a local anti-virus program to install and configure an application locally).
- Users shall not be allowed to install software. Only IT Support staff shall be allowed to install approved software, in accordance with IT ASSET STANDARDS.
- The Group shall minimize malware risks by backing up critical information, in accordance with IT DISASTER RECOVERY
- IT Support staff shall periodically (once a week is recommended) review all anti-virus, firewall and other relevant logs to determine if the software is up-to-date and is performing as expected. Tech Support shall report its findings to the IT Security Manager for possible action.

- The IT Security Manager shall periodically (monthly, at a minimum) review security incident information (IT INCIDENT REPORT and IT THREAT ASSESSMENT REPORT) to determine incident trends and progress toward Group goals. IT Management shall periodically (annually, at a minimum) meet with the IT Security Manager to review the Malware Defense Plan, to determine its continuing applicability and conformity to Group requirements. In the event that anti-malware measures do not prevent malware from infecting any part of the IT network, that event shall be handled in accordance with IT INCIDENT HANDLING.

Computer Viruses

For the purpose of preventing infection by and spread of, computer viruses, the following controls and precautions are mandatory:

- Desktop computers should be equipped with virus detection software, which enables automatic updates
- Users should ensure that they shut down and power up their computers connected to the network, at least once a week, so as to receive virus signature offers and OS patches & updates
- Users should ensure that the virus detection software for laptops, which are not connected regularly in the office, is regularly updated
- Users should promptly report software / device malfunction or virus infection.

Remote Access Policy

Policy Statement - As a general rule, remote access to the NIGERIAN STOCKBROKERS LIMITED network shall be restricted and may only be granted on a need only basis with justification and approval by the Group Head, IT & operations

Remote Access Standards

The following requirements and standards must be adhered to:

- At no time should any NIGERIAN STOCKBROKERS LIMITED employee provide their login or email password to anyone not even family members.
- NIGERIAN STOCKBROKERS LIMITED employees and contractors with remote access privileges must ensure that their NIGERIAN STOCKBROKERS LIMITED-owned or personal computer or workstation, which is remotely connected to NIGERIAN STOCKBROKERS LIMITED's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- NIGERIAN STOCKBROKERS LIMITED employees and contractors with remote access privileges to NIGERIAN STOCKBROKERS LIMITED's corporate network must not use non-NIGERIAN STOCKBROKERS LIMITED email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct NIGERIAN STOCKBROKERS LIMITED business, thereby ensuring that official business is never confused with personal business.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Non-standard hardware configurations must be approved by IT Security Team and IT must approve security configurations for access to hardware.
- All hosts that are connected to NIGERIAN STOCKBROKERS LIMITED internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.
- Personal equipment that is used to connect to NIGERIAN STOCKBROKERS LIMITED's networks must meet the requirements of NIGERIAN STOCKBROKERS LIMITED-owned equipment for remote access. Organizations or individuals who wish to implement non-standard Remote Access solutions to the NIGERIAN STOCKBROKERS LIMITED production network must obtain prior approval from IT Security Team.

INFORMATION SECURITY – ACCESS & CLASSIFICATION POLICY

Overview

The company originates and deals with varied information in electronic and printed form. To ensure adequate security is applied to all information in our possession, they should be classified according to import and value with all information having an identifiable owner. Definitions

Term	Definition
NDA	Non-Disclosure Agreement
SA	System Audit
IC	Internal Control
IT	Information Technology

Scope

This policy applies to all NIGERIAN STOCKBROKERS LIMITED staff and vendors; it covers information generated by the company both electronic and printed.

Policy Statement

Access to all information held by the company will be granted on a need-to-have and need-to-use basis. The owner of information will be taken as the originator of the information or the owner of the application that produces stores or processes the information. All staffs

are responsible for the security of information and systems entrusted to them by the company.
The classification of information and systems will determine the level of security that will be applied to protect it. Systems must be classified according to the total value of information that they support.
Information classification
In applying classifications, the primary consideration should be the gravity of compromise to the company or the persons involved. Information originators should be careful not to under or over classify information because of the attendant consequences. All information held by the company shall be classified in one of the four categories below:

- Highly Confidential: This will be applied to information that could extensively damage the company, its employees or its customers if it is lost, disclosed or modified. Only a very small amount of the company's information will fall into this category. Highly Confidential documents will normally contain information which, if compromised, could: Place personnel at risk, Influence the share price of the Company and/or other companies, Prejudice management strategy, Adversely affect the company's reputation, Cause the company serious financial loss or Prejudice litigation.
- Confidential: This applies to information that could be detrimental to the company, staff or customers if it is lost, modified or leaked. This includes information which, if compromised, could negatively affect the effectiveness of management or breach confidentiality agreements. Information held by the company‘s core companying and supporting systems will be classified as confidential.
- Private: This applies to information which, if disclosed, may breach personal privacy or cause employees‘ embarrassment; matters concerning an employee's health, family, discipline, promotion, salary or appraisal, etc. will fall into this.
- Internal Circulation: This refers to information not intended to be disclosed outside the company.

Information that does not justify a classification of —Internal Circulation will be covered by the oath of secrecy taken by each staff; this information will still be accorded reasonable protection to prevent access by third parties.
A criticality rating of systems into Critical, Important or Low will be carried out, according to whether the highest rating of the information confidentiality, integrity or availability is high, medium or low respectively. The degree of protection to be accorded each system will be determined by its criticality rating; this rating will be carried out by business owners in conjunction with IT Group.

Granting access to information
Access to information classified as Highly Confidential, Confidential or Private will be authorized by the information owner or any other persons delegated with that authority.
Enforcement
Implementation of this policy will be verified from time to time by IC and SA. Any employee found to have violated this policy shall be subject to disciplinary action including termination of employment.
User Management
User On-Boarding Process

To ensure that all personnel in the employment of NIGERIAN STOCKBROKERS LIMITED are aware of the threats and concerns, and are equipped to support information management policy, standards and guidelines in the course of their normal work, all users of computing facilities in NIGERIAN STOCKBROKERS LIMITED and subsidiaries are required to attend a mandatory Information Security training within the first two months of their engagement.
The Information Security and Assurance Officer will regularly advise relevant training, delivery mode and completion timeline.

Disengagement Process
To ensure that all personnel leaving NIGERIAN STOCKBROKERS LIMITED return their assigned items (such as laptop, mobile phone, documents, keys and security badge) and to ensure that their building and IT access rights are revoked prior to leaving the site. The disengagement checklist in use by HCM must include list of recoverable items from all staff.
Recoverable IT items must be returned to the IT Service Manager (or his nominee) after which the necessary forms will be signed.
Handling Desktop Computers and Information All staff and contractors are responsible for proper use of Desktop Computers. For the purpose of this policy "Desktop Computer" is a term used to cover NIGERIAN STOCKBROKERS LIMITED approved equipment such as personal computers, workstations, docking stations, portable computers, modems, or other data processing desktop hardware. Each use is personally responsible for the control of this equipment, including the installed software.

For the purpose of avoiding breach of statutory or contractual requirements, knowing fully well that use of software that has been illegally acquired can lead to legal action, and perhaps criminal proceedings, against NIGERIAN STOCKBROKERS LIMITED, all users of NIGERIAN STOCKBROKERS LIMITED desktop computers must ensure that only software developed, or acquired, through approved NIGERIAN STOCKBROKERS LIMITED procedures may be installed on NIGERIAN STOCKBROKERS LIMITED

Laptop and Desktop computers.

Policy Statement
All NIGERIAN STOCKBROKERS LIMITED data must be protected against loss.
All NIGERIAN STOCKBROKERS LIMITED staff and where applicable IT Support Staff should:

- Make regular backups of data stored on the local hard disk (if applicable).
- Secure all diskettes, tapes, CD-ROMs and other computer readable media to prevent theft, loss or corruption; using centrally managed safe storage facilities when appropriate.
- Secure own Desktop computer with a physical key and/or reliable login password.
- Protect passwords, change them regularly, do not pass them on or share them with others, preferably choose a combination of letters and numbers that is difficult for others to guess.
- Ensure that if the Desktop computer is left unattended for a long period it is either switched off or locked with a screen or keyboard-locking device. Report security incidents (virus, hacking, theft, etc.), suspected weaknesses or software malfunction immediately to the IT Help desk. 6.16 Identity Management

All employees of NIGERIAN STOCKBROKERS LIMITED are responsible for managing assigned unique user IDs and passwords. The use of a unique ID helps ensure accountability and easy tracing of transactions to individual person(s) through an audit trail. However when an individual's user ID which is tied to an individual's role/ privilege/ profile is compromised, this can result in fraud and losses in the business, both in terms of financial loss but also loss in productivity. It is therefore important that all employees follow good security management practices by not disclosing user ID's and passwords to unauthorized persons, staff and colleagues. On no basis should a user disclose his / her password. Techniques such as social engineering, phishing are common in the business environment. This techniques are commonly used in gaining unauthorized access to individuals user names, password, PIN, etc. On no occasion should a staff / customer disclose this. If in doubt, kindly speak with the Information Security Officer / Advisor for guidance.

Overview
There are three strong reasons for formulating and implementing a clear desk policy, each of which is grounded in the NIGERIAN STOCKBROKERS LIMITED good business practice and principles:

- To prevent information from getting into wrong hands
- To protect company and personal belongings from theft
- To promote good housekeeping

Enforcement of the Clear Desk policy is of interest to Information Security for the purpose of protecting business information and data, but compliance verification will be left to IC for enforcement. Notwithstanding, user education on this will be undertaken as and when necessary.

Access by Third Parties to NIGERIAN STOCKBROKERS LIMITED IT Infrastructure
Infrastructure Access to NIGERIAN STOCKBROKERS LIMITED IT Infrastructure by Third Party Companies or Contractors and their personnel is allowed subject to the following:

- A Third Party access request form must be completed for the Third Party user. The request, in addition to other necessary details, must state the Business activity requirements (and associated necessary systems, applications, permissions and authorities), scope of permissions required, scope of authority and Limitations. The request must be sponsored by a department / unit in the NIGERIAN STOCKBROKERS LIMITED or and duly approved by the departmental head/ delegate.
- An IT Security agreement must be signed with the Third Party organization. This can be documented as part of the Contract document for the job or as a separate IT Security agreement.
- The individual account users shall be limited to the applications (or relevant portion) and system required only. Where this is not possible, then the account shall not be created.

Access to the Internet
Access to the Internet via NIGERIAN STOCKBROKERS LIMITEDIT infrastructure will be for business purposes only. Employees and others provided access to the Internet must take every precaution to guard company intellectual property, protect network integrity and prevent legal liability.
2.20 Access to the Internet by Third Parties Access to the Internet via NIGERIAN STOCKBROKERS LIMITED facilities may be granted to Third Parties (contractors, consultants and business partners). Authorization for access will be part of the general access policy. All NIGERIAN STOCKBROKERS LIMITED information security policies and procedures will apply, and the third party must be made fully aware of these policies and procedures and their responsibility for compliance.
For more information on the internet policy, refer to the NIGERIAN STOCKBROKERS LIMITED Computer and Internet usage Policy.

Information Security Education

All users of computing facilities in NIGERIAN STOCKBROKERS LIMITED must receive Information Security training in organizational policies and procedures to ensure they are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of normal work.

Physical Security and Access Control

To maintain appropriate protection of organizational assets, all information and communication infrastructure must be protected against unauthorized access and configuration changes.

Asset Inventory

To maintain appropriate protection of organizational assets, all IT assets must be documented have a nominated owner or action party for compliance and support. Accountability for assets helps to ensure that appropriate protection is maintained. The list of inventories must be maintained.

User Account Management Policy

Policy Statement

Provision of Access to Information must be fulfilled before a user account is created in order to prevent unauthorized access to information, systems and computing services.

User Account Creation Process

To create a user account the following process should be followed:

- User/requester will raise an account creation request and forward to own Supervisor (or his/her designate) for approval. Use of an email or hard copy form is also allowed for both request and approval. Where a high-privilege, admin or support account is required, the justification for the request must be clearly documented as part of the request.
- All requests are required to be approved by the requester's Supervisor, his designate or anybody in the Line hierarchy above the Supervisor.

User Account Termination Process

User accounts must be promptly revoked when no longer required, particularly upon staff / contractor disengagement, to forestall unauthorized access to the system. To facilitate prompt account termination, HR will send list of disengaged staff to IT who will then disable / delete such user account from the network and system respectively.

User Account Reconciliation

User accounts must be regularly reviewed to establish dormant accounts with a view to disabling such. For this purpose, IC and SA shall review user account and logon activities periodically to establish dormant accounts with a view to disabling such. It is recommended that this review be carried out on a monthly basis (although quarterly review is also allowed) Information Security Incident Reporting and Response The objective of a security reporting and response process is to protect against security threats/risks and minimize damage to the business from security incidents. Security incidents require immediate action to contain the damage and to restore IT services as soon as possible. The knowledge gained from the follow-up of incidents also help to define the right level of protection for the future.

An Information Security Incident can take many forms and can be indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. For the purpose of the NIGERIAN STOCKBROKERS LIMITED Information Security Incident Management, an Information Security event can be located within the frame of an attempted or successful unauthorized:

- Access, use, theft, disclosure, modification or destruction of information or Interference with or misuse of information processing infrastructure
- Or a significant warning that such activity may be imminent.

Disposal of information assets

All data storage media used for storing business critical data shall be checked by the relevant department and IT to ensure any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Techniques such as degaussing are highly recommended for deleting information on computer hard disk drives. Disposal of information assets is not limited to electronic data only but covers sensitive hard copy documents which may be confidential and should not be available to unauthorized persons. Adequate measures should be put in place for the secure disposal of hardcopy documents.

Duties and responsibilities of staff shall be segregated to reduce the risks of unauthorized or unintentional modification or misuse of the Group's assets.

Segregation of Duties ensures no staff has the ability to single handedly process a transaction end to end. This would help ensure and reduce the risk of fraud by timely detecting unauthorized activities when a transaction is processed.

Enforcement

Implementation of this policy will be verified from time to time by IT, IC and SA. Any employee found to have violated this policy shall be subject to disciplinary action including termination of employment.

IT Backup and Retention Policy

In information technology, a backup or the process of backing up refers to making copies of data so that these copies may be used to restore the original data or information after a data loss event.

Backups are useful primarily for two purposes.

The first is to restore a state following a disaster (called disaster recovery).

The second is to restore small numbers of files after they have been accidentally deleted or corrupted and prevent data loss.

The need to backup business critical data is largely borne out of the need to be able to provide business continuity and ensure that line of business applications and systems can be restored to full operation from a disaster or crisis without causing significant loss to the business.

In the light of that, Return Point Objective and Return Time Objectives which are critical factors which determine significant aspects of the backup strategy, approach and technology are determined strictly by business and regulatory requirements. Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users.

Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time.

The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. The recovery grid below describes the Priority of each data category based on the RTO and RPO as defined by business requirements.

Considerations

Since a backup system contains at least one copy of all data worth saving, the data storage requirements are considerable. In the modern era of computing there are many different types of data storage devices that are useful for making backups. The storage device options usable are however limited by specific technology capabilities and requirements in our local environment. The goal however, is to ensure that whichever storage device used provides geographic redundancy, data security, and portability.

For the purpose of the IT environment within NIGERIAN STOCKBROKERS LIMITED, we will be using a combination of a Full and incremental application and data Backup model. This type of backup is designed to allow an entire system to be recovered to the point at which the last backup was taken.

A full system backup makes a complete image of a systems application and databases while an incremental backup makes a copy only of changes in data; if needed, these backups can be copied back to the same or a different system to ensure minimal data loss.

Policy Scope

This policy applies to all Information Technology services and applications supported by the IT group of NIGERIAN STOCKBROKERS LIMITED and their dependencies. It also applies to all services supplied by external vendors which are hosted within our environment.

Policy Statement

All Priority 1 and Priority 2 applications, data and file systems will be regularly backed up using media provided and the backups retained for the periods agreed in this policy document.

All applications and services have been categorized based on the recovery grid detailed above into 2 broad categories:

Priority 1 Applications

These are services which impact directly on business processes and customer relationship management. These typically refers to transactional and communication applications.

Priority 2 Applications

These are services which impact on internal enterprise enablement, management and control systems with no direct or negligible cost impact on the business. The retention period for which all application and data backed up is determined primarily by the business impact of the application or service. The following table shows the application, categorization and the corresponding backup and retention requirements.

Priority 1 Applications

Application software Core Company System Backup Type Frequency Media Retention Data Integrity Check Full Database Once Daily before and Once Daily Tape One Month Monthly after End of Day

Full Database Once Monthly before and Twice Tape Forever Quarterly Monthly after End of Month

Full Application Once Monthly after End of Month Tape Forever Quarterly Postilion/FEP Backup Type Frequency Media Retention Data Integrity Check Full Database Weekly Disk One Week Monthly Incremental Daily Disk One Week Monthly database

Full Database and Monthly Disk & One Month Monthly Application Tape Exchange Backup Type Frequency Media Retention Data Integrity Check Full Database and Weekly Disk One Month Monthly Mailbox

Incremental Daily Disk One Week Monthly database and

Mailbox

Full database and Monthly Disk & One Month Monthly mailbox Tape Third Party Transactional Applications Backup Type Frequency Media Retention Data Integrity Check Full Database Weekly Disk One Month Monthly Incremental Daily Disk One Week Monthly database
Full database and Monthly Disk One Month Monthly Application and Tape

Priority 2 Applications
Internet Companying Backup Type Frequency Media Retention Data Integrity Check Full database Weekly Disk One week
Quarterly Full database and application Monthly Disk & Tape Monthly Quarterly Data Warehouse Backup Type Frequency Media
Retention Data Integrity Check Full database Weekly Disk One week Quarterly Incremental database Daily Disk One week
Quarterly Full database and application Monthly Disk One Month Quarterly In-House Developed Applications Backup Type
Frequency Media Retention Data Integrity Check Full database Weekly Disk One Week Quarterly Incremental database Daily Disk
One Week Quarterly Full application and Database Monthly Disk & Tape One Month Quarterly Third Party Non-Transactional
Applications Backup Type Frequency Media Retention Data Integrity Check Full database Weekly Disk One Week Quarterly
Incremental database Daily Disk One Week Quarterly Full application and Database Monthly Disk & Tape One Month Quarterly.

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.

BUSINESS CONTINUITY / DISASTER RECOVERY PLANNING

The purpose of business continuity/disaster recovery is to enable a business to continue operations in the event of a disruption and to survive a disastrous interruption to their information system. Rigorous planning and commitment of resources is necessary to adequately plan for such an event. Business continuity planning (BCP) is a process designed to reduce the organization's risk for an unexpected disruption of the critical functions/operation (manual or automated) necessary for the survival of the organization.

This includes human/material resources supporting the critical functions/operations, and assurance of the continuity of the minimum level of services necessary for critical operations.

Information Systems Business Continuity Planning/Disaster Recovery plans

Information systems business continuity/disaster recovery planning is a major component of an organization's overall business/disaster recovery plan. Information systems processing is of strategic importance, because almost all business processes are dependent on the use of automated information resources because almost all business processes are dependent on the use of automated information resources to achieve an organization's mission objectives, therefore, there should be a ready-to-start reserved facility to support these key operations in case of a disruption.

When separate, information system plans must be consistent with and support the corporate business continuity plan.

Disasters and Other Disruptive Events

Disasters are disruptions that cause critical information resources to be in operative for a period of time adversely impacting business operations. The disruption could be several hours to several days, depending upon the criticality of the information resource. Most importantly, disasters require action to recover operational status.

A disaster may be caused by natural, calamities, like earthquakes, floods, tornados, severe thunderstorms, fire etc., which cause extensive damage to the processing facility and the locality in general.

A disaster also could be caused by events caused by human beings like terrorist attacks, hacker attacks etc.

The business continuity planning process can be divided into the following phases;

- ➔ Business impact analysis
- ➔ Develop business recovery strategies
- ➔ Develop detailed plan
- ➔ Implement plan
- ➔ Test and maintain plan

Business Risk: - Potential for harm or loss in achieving business objective

The Risk Assessment Phase

The risks identified with our operations are stated below:

1. Fraud: the crime of deceiving in order to get money or goods illegally. Verify/confirmation of any documentation and make sure it is duly authorize. Restrict access to sensitive documents. Control over data input procedures.
2. Sabotage: disgruntled staff or business competitors can cause this. Identify such disgruntled staff, and remove staff from sensitive position, i.e. cash and employees who are mentally unstable
3. Disaster; - this is classified into fire, flooding, lightning and earthquakes

- The computer equipment is comprehensively insured and the insurance policy kept in the custody of an authorized official.
- No smoking regulations in machine room
- Hand – held manual fire extinguishers
- Documented fire emergency procedures

4. Exposure of Sensitive Information: Utilizing the organizations data to obtain favour.
5. Systems Abuse; This can be attributed to using the system for personal use, or unauthorized transactions.
6. Virus Infection on PCs; - Virus scan diskettes/before use

- The floppy drive on the PCs should be disabled.
- Workstations kept outside the computer should be of diskless type.

7. Data entry/Operation Errors; - Control over data input procedure

- Separation of operations from other activities
- Maintenance of operational trouble log; to avoid mistake done in the past

8. Inventory and other material frauds; - system for limiting physical access to the computer room and other sensitive area.

Business Impact Analysis

Business impact analysis (**BIA**) is one of the key steps in developing the business continuity plan. This phase involve identifying the various events that could impact the continuity of operations and their impact on the organization.

Business Recovery Strategies

The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from disaster. A recovery strategy identifies the best way to recover a system in case of disaster and provides guidance based on which detailed recovery procedures can be developed.
The recovery strategies can be placed into three possible scenarios:

(a) Pre-determined
(b) Pre- arranged
(c) Redundant

Pre-determined Recovery Strategy

This strategy assumes that a given resource can be obtained from given sources in a very short time without the aid of a binding contractual arrangement.

Pre-arranged Recovery Strategy

This is a modification of the pre-determined recovery strategy, with a written contract spelling out the conditions for the attainment and use of a particular IT resource component eg Computer hot site.
Redundant Recovery strategy

This strategy delineates the securing of an exact duplicate of a given IT component so that backup and restoration can be immediate and identical to the system, as it existed prior to the disruption.
Names and Addresses of Service Providers, backup up equipment suppliers

Name of Organization	Addresses	Conta
Zastmedia	16, Amodu Ojikutu Str, Victoria Island, Lagos	Esther
InfoWARE	AIICO Plaza, Plot 12 Churchgate St;, Victoria Island, Lagos	Omow
Allied Computers	227, Ikorodu Road, Ilupeju, Lagos.	Adeso
21st Century Limited	Plot 249A Muri Okunola Street, V.I Lagos	Azeez
Improved Power Source Limited	23A Fatai Atere Way, Matori Lagos	Abdul
VSR Solutions	4b, Alhaji Bello Str. Off Airport Rd, Ikorodu, Lagos	Mr. Er

Recovery Schedule
The organization has signed an agreement with Montgomery Vaults for the use of deposit box and a mini-vault to store backup computer equipment's and data.
Montgomery Security Vaults (Nig) Ltd operates the first private offsite depository in Black Africa with physical features specifically designed and built to the highest International standards and specification.
Montgomery Security Vaults (Nig) Ltd was created by eight of the Largest Insurance Corporations in Nigeria along with some other investors to provide absolute confidentiality in private depository and safe storage for corporate bodies and individuals. This company is located at No, 25 Montgomery Road Yaba Lagos.
The mini-vault is opened only by numbered combination lock. These numbers (maximum 6 digits) were selected by the organization and only known to the organization, once the door of the vaults is locked, Montgomery security vault cannot open it. The combination lock and the spare key of the computer box are in the custody of the Head Operations Management.
There is a certificate to show that during the life of the said Rental Agreement and any renewal thereof, or

until further notice from the Organization, the following agents and officers of the organization are hereby authorized to have the access as joint depositors to the said vaults/box and the control of the contents thereof.

Authorized Depositors

NAMES OF STAFF

1. Head, IT
2. Head, Compliance
3. Head, Risk Management

Provided that at least two of the said agents and officers shall attend whenever access is to be had to the said box.

Information Systems Recovery Activities

Activity	Contingency Envisaged	Likely effect
Directory of each contact support persons for all hardware and software	Systems failure	Hardware application failu
Early End of Day	Systems failure after the days run	Hardware/Software failur
Report Generation	System failure after midnight	Hardware or Software fail
Full System Back-up	Hardware/Software failure	Communication/NITEL fai l
SWIFT messaging system	Communications/NITEL failure	No SWIFT messages in going
	Interface failure	No SWIFT messages outgoing
	SITA failure	NO swift messages in or o
	SWIFT Network is unavailable	No Swift messages in or ou
BASIS Organizationing Application	System failure requiring switch over to manual operations	All operation to be manually
Workstation	System failure power problem	Inability to post transactio
LAN	Systems failure	Inability to distribute co resources

Periodicity of Test of Backup

Testing strategy for Offsite Backup

Specification of how the tests would be conducted including details of stages, test, data and files expected result

TEST TABLE

DATE	DESCRIPTION
	Restore the data for January-end
	Restore the data for February-end
	Restore the data for March-end
	Restore the data for April-end
	Restore the data for May-end
	Restore the data for June-end

Periodicity of test backup –register should be maintained at the offsite, site.

ALTERNATIVE STRATEGIES

- BACKUP AND RECOVERY
- Arrangements for alternative data processing
- Hardware
- Software
- Personnel
- Supplies

<- Backup plan

- The following issues should be clear in backup plan
- Which data are most important?
- How much protection is too much?
- Where is it safe to keep backups?
- How will you the backups be tested?
- What kind of archiving is necessary?

DISASTER RECOVERY STRATEGY

The disaster recovery strategy explained below pertains specifically to a disaster disabling the main computer room. This provides computer and major server support to **NIGERIAN STOCKBROKERS LIMITED** applications. Especially at risk are the critical applications those designated as Category I (see below) systems. The Business Continuity Plan complements the strategies for restoring the data processing capabilities normally provided by Operations & Systems.

This section addresses three phases of disaster recovery:
· Emergency
· Backup
· Recovery
Strategies for accomplishing each of these phases are described below.

Emergency Phase

The emergency phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures of Fire Wardens and Admin Department direct efforts to protect life and property, the primary goal of initial response. Security over the area is established as local support services such as the Police and Fire Departments are enlisted through existing mechanisms. The BCMT members are alerted by phone and begin to monitor the situation.
If the emergency situation appears to affect the main computer room (or other critical facility or service), either through damage to data processing or support facilities, or if access to the Tower is prohibited, the Duty Person will closely monitor the event, notifying BCMT personnel as required assisting in damage assessment. Once access to the facility is permitted, an assessment of the damage is made to determine the estimated length of the outage. If access to the facility is precluded, then the estimate includes the time until the effect of the disaster on the facility can be evaluated.
If the estimated outage is less than _3_ hours, recovery will be initiated under normal Information Systems operational recovery procedures. If the outage is estimated to be longer than _72_ hours, then the Duty Person activates the BCMT, which in turn notifies the Group head Information Technology Department and The Managing Director and the Business Continuity Plan is activated. The recovery process then moves into the back-up phase.
The Business Continuity Management Team remains active until recovery is complete to ensure that the Organization will be ready in the event the situation changes.

Back-up Phase

The back-up phase begins with the initiation of the appropriate Plan(s) for outages enduring longer than _72_ hours. In the initial stage of the back-up phase, the goal is to resume processing critical applications. Processing will resume either at the main computer room or at the designated site, depending on the results of the assessment of damage to equipment and the physical structure of the building.
In the back-up phase, the initial site must support critical (Category I) applications for as long as possible and as many Category II applications as resources and time permit. During this period, processing of these systems resumes, possibly in a degraded mode, up to the capacity of the site.

Recovery Phase
The time required for recovery of NIGERIAN STOCKBROKERS LIMITED Towers and the eventual restoration of normal processing depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with back-up operations at the designated site. The primary goal is to restore normal operations as soon as possible.
1. Function
To provide for all facets of a positive security and safety posture, to assure that proper protection and safeguards are afforded all NIGERIAN STOCKBROKERS LIMITED employees and assets.

- Identify fire exit points
- Directs occupants to move to assembly points
- Educate occupants to use fire exit staircase and avoid the use of lifts
- Ensure evacuation is done steadily and in an orderly manner
- Ensure pregnant, disable or sick people are assisted and all other occupants vacate at the time of the alarm.
- Ensure some staff are dedicated to help with the children in the Crèche.
- Ensure nobody returns to the building until roll call is over
- Take roll call at the muster point
- Fight fire with available fire fighting equipment
- Inform Federal Service on tel. no. 119or 199 (Lion Building) or D/L 2633355

2. Organization
The team will consist of the Fire Wardens and appropriate support staff. The team will report through the Head Material Resources Department who is a member of the Business Continuity Management Team.
3. Interfaces
The Fire Wardens Team will interface with the following teams units, relative to security and safety requirements:
Personnel
GIS Department
Corporate Affairs
Engineering unit of the Management Consultants to the building
4. Preparation Requirements
Identify the number of Fire Wardens personnel needed to provide physical security protection of both the damaged and backup sites.
Identify the type of equipment needed by Fire Wardens personnel in the performance of their assigned duties.

Coordinate and arrange for additional security equipment and manpower, as applicable, if needed.
Periodically hold meetings to keep abreast of information on procedural changes.

Corporate Affairs - Public Information

1. Function

The most difficult time to maintain good public relations is when there is an accident or emergency. A public relations planning is required so that when an emergency arises, inquiries from the news media, friends and relatives of staff, and customers can be handled effectively. While we cannot expect to turn a bad situation into a good one, we can assist in making sure facts presented to the public are accurate and as positive as possible given the situation.

It is in our best interest to cooperate with the media as much as possible, so that they will not be forced to resort to unreliable sources to get information that could be untrue and more damaging to the Organization than the facts.

Therefore, it is the policy of NIGERIAN STOCKBROKERS LIMITED in time of emergency, to:

Have the Head Corporate Affairs serve as the authorized spokesperson for the Organization. All public information must be coordinated and disseminated by the department. Refrain from releasing information on personnel casualties until families have been notified. Once families have been notified, names of those personnel should be released quickly to alleviate the fears of relatives of others.

Provide factual information to the press and authorities as quickly as facts have been verified, and use every means of communications available to offset rumors and misstatements.

Avoid speculating on anything that is not positively verified, including cause of accident, damage estimates, losses, etc. (Fire Officials normally release their own damage estimates.)

Emphasize positive steps taken by the Organization to handle the emergency and its effects.

Situations calling for a statement from Corporate Affairs may include, but are not limited to: Systems malfunction disrupting the normal course of operations.

Accidents, particularly when personal injury results.

Natural disasters, such as fires, floods, tornadoes and explosions.

Civil disorders, such as riots and sabotage.

Executive death.

Scandal, including embezzlement and misuse of funds.

Major litigation initiated by or against the Organization.

2. Organization

The Head Corporate Affairs, a member of the Business Continuity Management Team, will act for the Organization. In his absence the responsibility will revert to the next Senior Staff in the department.

3. Interfaces

The Corporate Affairs will be the interface between NIGERIAN STOCKBROKERS LIMITED and the public or news media. Copies of all status reports to the Business Continuity Management Team or Computer Users Monitoring Committee will be forwarded to Corporate Affairs for potential value in information distribution for good public relations. They will work with the HRM in dissemination of information to staff.

4. Preparation Requirements

Existing relationships with local media will be utilized to notify the public of emergency and recovery status. The Head Corporate Affairs will maintain up-to-date contact information for the media and other required parties.

A facility will be identified to be used as a pressroom.

Arrangements will be made to provide the necessary equipment and support services for the press.

Insurance

1. Function

To provide for all facets of insurance coverage before and after a disaster and to ensure that the recovery action is taken in such a way as to assure a prompt and fair recovery from our insurance carriers.

2. Organization

The team will consist of the Head Material Resources Department and required staff and insurance carrier personnel i.e. STERLING INSURANCE BROKERS LTD. The team reports through the Business Continuity Management Team, of which it is a member.

3. Interfaces

The Insurance Team will interface with the following teams, relative to insurance matters:

Corporate Affairs

Fire Wardens

Damage Assessment/Salvage

Information Systems Department

Sterling Insurance Brokers Limited

This team will be activated upon the initial notification of a disaster.

4. Preparation Requirements

Determine needs for insurance coverage. Identify the coverage required for hardware, media, media recovery, liability and extra expense.

Prepare procedure outlining recommended steps to be followed by Damage Assessment/Salvage Team during initial stage of disaster

Arrange for availability of both still and video recording equipment to record the damage.

Ensure that an equipment inventory is available, to include model and serial number of all devices.

Evaluate all new products and services offered by NIGERIAN STOCKBROKERS LIMITED for potential liability in the event of a disaster.

Telecommunications / Networking

1. Function
To provide voice and data communications to support critical functions. Restore damaged lines and equipment.

2. Organization
The team will consist of appropriate Technology staff that will also coordinate with and supervise outside contractors as necessary. The team will report through the Head Technology, who is a member of the Business Continuity Management Team.

3. Interfaces
Technology will interface with the following departments, relative to telecommunications requirements:
Admin Department
Other Information Systems department staff as necessary
Other NIGERIAN STOCKBROKERS LIMITED departments requiring emergency telecommunications
Outside contractors and service providers as necessary

4. Preparation Requirements
Provide critical voice and data communications services in the event that normal telecommunications lines and equipment are disrupted or relocation of personnel is necessary.
Consult with outside contractors and service providers to ensure that replacement equipment and materials are available for timely delivery and installation.
Utilize available resources, to broadcast information relevant to the disaster.

PART IV. RECOVERY PROCEDURES
Notification List
This appendix contains the names of managers and personnel who must be notified in the event of a disaster. The Business Continuity Management Team Coordinator is responsible for keeping this notification list up-to-date.

Computer Users Monitoring Committee Secretariat
Managing Director
Vendors e.g. Allied Computers
Business Continuity Management Team Co-coordinator

Admin department is assigned responsibility for the interface with other staff to monitor emergencies as they occur. These Early Warning Duty people are then responsible for activation of the full Business Continuity Management Team and necessary NIGERIAN STOCKBROKERS LIMITED Recovery Management Teams.

Business Continuity Management Team Coordinator
This appendix contains instructions to the Business Continuity Management Team Coordinators for overseeing disaster response and recovery efforts.

Action Procedures
Player Action
Coordinator Ensure entire Business Continuity Management Team (BCMT) has been notified. Then notify Chairman of Computer Users Monitoring Committee.

Coordinator Activate the Emergency Operations Center at the Car Park and notify staff to meet there.

Coordinator Meet with Damage Assessment Team to review their findings and present results to BCMT.

Coordinator Present recommendations to BCMT for next steps in recovery effort.

Coordinator Begin notification of all recovery teams. Check to ensure all recovery participants have been notified.

Coordinator Monitor the activities of the recovery teams. Assist them as required in their recovery efforts.

Coordinator Report to BCMT on a regular basis on the status of recovery activities. Report to Computer Users Monitoring Committee as appropriate on recovery status.
Coordinator On an hourly basis, or other appropriate interval, updates the Organization through HRM and Corporate Affairs.

Damage Assessment/Salvage
This appendix contains instructions to the Damage Assessment/Salvage Team for disaster response and recovery efforts.

Action Procedures
Player Action
Building Services Notify the Management Consultants to the building, team members, and vendors to report to the site for initial damage assessment and clean up.

Admin Department Notify insurance representative Team Leader Request permission to enter site from Fire Department (if required). Take a service representative from each of the appropriate vendors; the insurance claims representative and appropriate Admin Department and Information Systems personnel into the site.

Team Members Review and assess the damage to the facility. List all equipment and the extent of damage. List damage to all support systems (power, A/C, fire suppression, communications, etc.).

Team Leader Notify the BCMT as to the severity of the damage and what can potentially be salvaged.

Team Leader Notify the BCMT if the area can be restored to the required level of operational capability in the required time frame.
Salvage Operations

Player Action
Team Leader Initiate the Emergency Notification List and have all members report to the Staging Area.

Salvage Team Have the Building Services Supervisor determines which equipment and furniture can be salvaged. Photograph all damaged areas as soon as possible for potential insurance claims.

Salvage Team **Important** ** *Prior to performing any salvage operation contact Insurance Team to coordinate with possible insurance claims requirements and appraisals.*

Have the Admin Department Supervisor and staffs start salvaging any furniture and equipment.

Based upon advice from Insurance Team and ISD, contact computer hardware refurbishes regarding reconditioning of damaged equipment
Team Leader Meet with the Business Continuity Management Team Coordinator to provide status on salvage operations.
Configuration List
A sample of the configuration and full equipment inventory report from the Fixed Asset Management Team or other automated equipment inventories should be in off-site storage.
Action Procedures
Player Action
Head Material Resources Department contacts appropriate Insurance people upon first advice of disaster.
Head Material Resources Department meets with Damage Assessment/Salvage team at site.
Head Material Resources Department goes through disaster scene with Damage Assessment/Salvage team and advice on matters relating to insurance and claims. Ensures that nothing is done to compromise recovery from insurance carrier. Photographs all applicable areas.
Head Material Resources Department File all appropriate claims forms with all involved insurance carriers.
Report status of claims activity to the Business Continuity Management Team.

Telecommunications/ Networking
This appendix contains instructions to the ISD for disaster response and recovery efforts.

Action Procedures
Player Action
HELP Desk Personnel Receives report of disaster from Fire Wardens and notifies appropriate ISD and other personnel.
Head Technology Oversees assessment of damage to telecommunications facilities. Directs contingency and recovery efforts. Provides updates to Business Continuity Management Team and NIGERIAN STOCKBROKERS LIMITED Management.
Operations and Admin arrange for voice and dial-up data communications services to support critical functions. Procures stock to repair or replace damaged equipment. Restores full services in a timely manner.
ISD provides data communications facilities or circuits to support critical functions. Assists with restoration of cable and wire plant, as needed. Assists other departments with relocation and restoration of data facilities.

Appendix A - Recovery Facilities
The following facilities have been identified as designated recovery sites for restoration of processing under the NIGERIAN STOCKBROKERS LIMITED Business Continuity Planning strategy.

GUIDE TO BCMT ACTIVATION
1. The first indication of a problem will probably be a phone alert from Admin Department. Unless it's obvious that the problem is long term and severe, wait 30 minutes (for things in the Operations Center to quiet down) and call the department. Tell them you're calling for the BCMT and get the latest status about the problem reported by the phone call.
2. Does the problem prevent normal access, occupation or usage of any part of any of the building, or does the disaster disrupt service provided by telephones, the network, or the computers servers?
If no, go back to sleep!
If yes, continue.
3. Will expected recovery of the affected area last into normal business hours?
If no, go back to sleep!
If yes, continue.
4. Does the Head Material Resources Department indicate that the disaster will affect all services?
If no, go back to sleep!
If yes, continue.
5. ACTIVATE THE BCMT!
Call the coordinators first:
If they can't be reached, call the BCMT members directly. The numbers are on the list attached. The BCMT has three possible assembly points:
If the problem is minor, meet in the Conference Room _

All other problems, meet in the Emergency Operations Center Car Park.

Compliance Department is the Co coordinator - 08023799077

Head Corporate Affairs / Admin is a member - 08075502403

Head HRM is a member - 08039400114

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

This 28th March, 2026

…….. ……

Company Secretary Director