MUTUAL

Professionalism• Dynamism• Integrity

Mutual Benefits Assurance Plc RC269837

IS Policy Document

INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT

Policy Name	Information Security Policy
Policy Number	ICT 001
Policy Version	Draft 1.0
Policy Owner	Mutual Benefits Assurance Plc
Effective Date	November 01, 2017

APPROVALS

This document has been reviewed and accepted by:

Name	Title	Signature	Date
Olusegun Omosehin	Managing Director/CEO		Oct. 23, 2017
Olayinka Ogundeji	AGM, Internal Audit		Oct. 23, 2017
Femi Fapohunda	Controller, Information Technology		Oct. 23, 2017
Emmanuel Ormane	Controller, Enterprise Risk Management		Oct. 23, 2017

Title	Signature	Date
Board Audit Committee		
The Board		

1 INTRODUCTION

The Management of MBA is committed to information security by creating and maintaining an environment that adequately protects its information assets from unauthorised use, modification, disclosure or destruction. Information Security is seen as the preservation of the following three (3) characteristics of information:

- Confidentiality – i.e. ensuring that information is accessible only to those authorised to have access.
- Integrity – i.e. safeguarding the accuracy and completeness of information and its associated processing methods.
- Availability – i.e. ensuring that authorised users have access to information and associated processing systems when required.

Additionally, when information is transmitted or communicated, the following security principles also need to be complied with:

- Authentication/Identification – This serves to ensure that the identity of the user/entity can be positively verified.
- Non-repudiation – This serves to ensure that the sender and/or recipient cannot deny sending or receiving the information concerned.

The information security policies set out in this document complies with ISO 27001 standards, the international standard for information security management. Adherence to these policies will safeguard the confidentiality, integrity and availability of the entity's information assets and help secure the interests of the entity, its employees, customers, business partners and other stakeholders.

1.1 THE IMPORTANCE OF INFORMATION ASSETS TO MBA

Information assets are vital assets of MBA and shall therefore be adequately protected against all risks. The protection of MBA's information assets is also critical to MBA's continuity. Accordingly, sufficient measures in line with business requirements and commensurate with risks shall be taken to protect these information assets against accidental or unauthorised modifications, disclosure and/or destruction, as well as to assure the confidentiality, integrity and availability of MBA's information assets.

1.2 WHY MBA NEEDS INFORMATION SECURITY

MBA's information assets are critical for the entity's survival. Therefore, MBA shall ensure that such information assets are adequately protected when used by all parties authorised to have access to these resources. Information Security is one of the entity's prime responsibilities in protecting and securing its information assets. This responsibility is shared by all employees of MBA, from the highest to the lowest level. It is every employee's duty to protect MBA's information assets during internal and external use. In addition, it is also their duty to conform to statutory and contractual requirements regarding MBA's information assets.

1.3 Management's Commitment to Information Security

The security (confidentiality, integrity and availability) of information (all forms) is key to MBA's successful discharging of responsibilities to its customers and stakeholders. Therefore, it is the responsibility of every employee to ensure the security of MBA's information, systems and programs that facilitate its use. In addition, every employee of MBA, including temporary staff (e.g. National Youth Service Corp and Industrial Training staff), contractors, service providers, and consultants utilising the entity's information assets shall be responsible for ensuring the confidentiality, integrity and availability of MBA's information assets.

The full support and commitment of management in enforcing information security in the entity is formulated in the policy statements outlined in this document. Management shall also be responsible for implementing controls throughout the organisation, in line with the corporate governance structure.

1.4 Scope

The purpose of this Information Security Policy is to specify the measures required to protect MBA's information assets from all types of threats, whether internal or external, deliberate or accidental. Specific policies, standards, procedures and guidelines to facilitate the implementation of this high level framework shall be established within groups and business units. However, these must align with MBA's corporate policy for Information Security.

1.5 Applicability

The Information Security Policy applies to MBA and all its employees, including temporary staff (e.g. National Youth Service Corp and Industrial Training staff), contractors, service providers, and consultants utilising MBA's information assets. The policy covers the entire corporate network including servers and personal computers (stand-alone or network-enabled) located at MBA Head Office and Branches. In addition the policy applies to systems that are under the jurisdiction and/or ownership of MBA, and all personal computers and or servers authorised to access MBA's corporate network.

1.6 Communication

The Information Security Policy will be communicated to all MBA employees, including temporary staff (e.g. National Youth Service Corps and Industrial Training staff), contractors, service providers, and consultants utilising MBA's information assets.

1.7 Review of Information Security Policy

The policy shall be reviewed when there are significant changes in the organization or at least once in a year. This is to ensure its continuing suitability, adequacy, and effectiveness. All standards and specifications are subject to revision, and all parties are encouraged to investigate the possibility of applying the most recent edition of the policies defined in this document.

2 ORGANISATION OF INFORMATION SECURITY

2.1 INTERNAL ORGANISATION

2.1.1 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

It is the responsibility of every user of MBA’s information assets to ensure that information security policies are being adhered to. However, for the purpose of accountability, there exists a structure in charge with ensuring that these policies are adhered to, and taking disciplinary actions in the event of deviation. The structure includes:

2.1.1.1 THE EXECUTIVE BOARD

The executive board gives authority to the Information and Communication Technology Office (which is the Information Security Office at MBA) to perform its role and is responsible for performing the following:

- Requiring that management sponsor the information security program, measure, monitor and report to the board on the effectiveness of the IS program.
- Providing resources for the implementation of information security initiatives and programmes including awareness campaigns in alignment with the entity’s strategy and risk profile.

2.1.1.2 SENIOR MANAGEMENT

Management shall be responsible for approving the Information Security initiatives and policies (including changes), strategies and budgets. In addition, senior management shall be responsible for performing the following functions:

- Providing direction and ensuring that Information Security initiatives and activities are aligned with business objectives and IT strategies.
- Actively overseeing and promoting the Information Security program
- Approving organisation wide actions to be taken where monitoring processes reveal significant deficiencies in controls or a need for additional security

2.1.1.3 INTERNAL AUDIT

To support the monitoring process, without losing independence, internal audit should:

- Develop approaches used to evaluate information risks
- Develop and maintain checklists used to evaluate the security vulnerabilities and threats
- Issue reports on information security-related audits and reviews
- Assist with the development of the monitoring process, for example to ensure that all key issues are addressed
- Have access to assessments of the current Information Security situation of the entity prepared by the Information Security Office (I,e the ICT office at MBA)
- Audit the Information Security Office function (I.e. the ICT office at MBA to ensure effectiveness.
- Monitor compliance with the information security policies

2.1.1.4 LEGAL

The Legal Team of MBA is responsible for ensuring legal applicability and enforceability of MBA's policies, standards and procedures, and ensuring that these policies, standards and procedures are aligned with legal, statutory, regulatory or contractual requirements.

2.1.1.5 Information Asset Owners

This refers to the functional heads and supervisors who supervise users and are accountable for particular information assets such as business applications. Information asset owners should:

- Review and approve all requests for access authorisations
- Initiate security change requests to keep security records accurate and up-to-date so they accurately reflect the users' roles and required access.
- Promptly inform the Information Security Office of employee terminations and transfers
- Provide the opportunity for training on business applications
- Initiate appropriate actions when problems are identified
- Follow existing approval processes within the organisation for the selection, purchase and implementation of any computer hardware or business application.

2.1.1.6 Head, ICT Department

The Head, Information and Communication Technology Department (ICT) has ultimate responsibility for information security at MBA and provides leadership and direction for the information security office. The Head, ICT provides an accurate view of the security condition of the entity and encourages 'information asset owners' to keep risks at an acceptable level. The Head, ICT's role includes the following:

- Act as a sponsor and advocate of the ICT Office
- Act as a sponsor of MBA's Information Security Program
- Implement the Board decisions on information security and ensure that security initiatives and activities are aligned with business objectives.
- Recommend Information Security budgets to Senior Management
- Act as a central point of ownership and management for enterprise-wide Information Security at the entity.
- Be in charge of determining the method and approach for implementing strategic Information Security objectives, initiatives, and directives.
- Monitor strategic initiatives within the entity to assess the impact on Information Security
- Get involved in strategic projects within the entity to ensure adequate Information Security management is taken into account and that projects comply with the entity's Information Security Policy.
- Ensure that weaknesses identified are addressed satisfactorily by the Strategic Business Units (SBU's).
- Perform Information Security Strategy development and maintenance
- Perform Information Security policies, standards, procedures and guidelines development and maintenance
- Monitor Information Security incidents within the entity
- Perform Information Security Planning and Management
- Perform proactive Security Management
- Provide training for Information Security Staff

- Liaison with Information Asset Owners

2.1.1.7 ICT OFFICER

The Information and Communications Technology (ICT) Officer provides day to day management of the Information Security Office. He/she will be responsible for the following:

- Execute MBA's Information Security Program
- Ensure compliance with security policies and report deviations
- Establish the overall Information Security user awareness strategy
- Co-ordinate business continuity testing and report findings to Head, ICT
- Establish and revise the corporate information security strategy, policy and standards
- Establish and co-ordinate appropriate working group forums to facilitate an organisation-wide representation, feedback, implementation and monitoring
- Recommend security measures to the Head, ICT and report information security activities at MBA to the Head, ICT;
- Report and evaluate changes to policies and standards;
- Implement, maintain and update MBA strategy, architecture, standards and procedures with input from all stakeholders;
- Ensure that all computer users are aware of the applicable policies, standards, procedures and guidelines;
- Coordinate awareness strategies and rollouts to effectively communicate security solutions in MBA;
- Establish and implement the necessary standards and procedures that support the Information Security Policy.

2.1.1.8 BUSINESS CONTINUITY TEAM

- Review the effectiveness of MBA's Business Continuity strategy and implemented Disaster Recovery controls;
- Coordinate Business Continuity Tests
- Review results of Disaster Recovery Planning
- Undertake Business Continuity documentation revisions
- Assist in Business Continuity implementation
- Act as Business Continuity coordinator in the entity

2.1.2 SEGREGATION OF DUTIES

There shall be a separation of conflicting responsibilities (such as the initiation and authorisation of critical business processes) so as to reduce the opportunity of fraud or unauthorised access to systems and/or assets. This shall be implemented in all business processes and applications belonging to MBA.

2.1.3 CONTACT WITH AUTHORITIES

There may be a requirement to establish points of contact with authorities such as the Nigerian Police Force (NPF) or the Economic and Financial Crimes Commission (EFCC). This will ensure that MBA has the right contacts in place if an incident occurs which has a requirement to involve or report to external authorities (e.g. where a security breach or crime is suspected or has actually occurred).

2.1.4 CONTACT WITH SPECIAL INTEREST GROUPS

The Head, ICT will identify and maintain the appropriate level of contact with Information Security special interest groups. This may involve ensuring that the entity is included on distribution lists of organisations that produce information security alerts and advice.

2.1.5 INFORMATION SECURITY IN PROJECT MANAGEMENT

There shall be information security reviews on all projects undertaken by MBA. These reviews are to ensure that the projects take into consideration the types of security breaches that could affect their individual processes, and shall have security enhancements to address such deviations. Issues raised and actions taken from the security reviews will be logged and tracked under the responsibility of the Head, ICT.

2.2 MOBILE DEVICES AND TELEWORKING

2.2.1 MOBILE DEVICE POLICY

This policy applies to all MBA employees, contractors, vendors and agents involved in service delivery who access MBA’s information assets using a non-MBA device. The policy includes the following:

- All devices used for processing and storing MBA’s information assets must be registered with the Entity.
- Only encrypted MBA issued devices will be used for mobile computing and storage. These devices must be updated with the latest antivirus definitions, operating system and security updates.
- Only MBA approved software shall be used in processing data.
- Information assets classified as **‘Public’** may be stored on personal devices. Information classified as **‘Confidential’** and **‘Highly Confidential’** shall not be stored or processed on personal devices without written approval from the Head of Department.
- Devices with access to MBA’s information assets shall not be left in possession of a non-MBA personnel.
- It is the user’s responsibility to take all necessary precautions to prevent loss of data, damage or theft of their mobile computing devices. If any issued device is lost or stolen it should be reported immediately to the ICT department as soon as possible in accordance with the information security incident management process.

2.2.2 TELEWORKING POLICY

This applies to remote access connections and connectivity being used to do work outside MBA. It also includes reading or sending email and viewing intranet web resources via any device used for remote access connectivity.

- Only MBA provided and configured communication links and Virtual Private Networks will be used to connect to the entity's internal network.
- Once authorised to work remotely on MBA equipment and data, it is the employees' responsibility to ensure that encryption facilities are available and operational on the equipment they are using.
- The ICT department should be contacted for advice or assistance if there are any doubts about the functionality of the encryption facility.
- When data records are processed remotely on non-networked systems, the data should be synchronised with the relevant centrally stored records as soon as possible.
- Systems used for remote, stand-alone processing should also be regularly taken into an office location and connected to the network to ensure that security tools and patches, including anti-virus programs, are correctly updated.
- Devices used to transport data should only contain the minimum data necessary, the data should be deleted from the device once it has been synchronised with the central records and is no longer needed on the portable device.

3 HUMAN RESOURCE SECURITY POLICY

3.1 INTRODUCTION

An integral part of MBA's information processing is its user-base. Personnel are exposed to information throughout their working day, some of which may be confidential or business critical. MBA needs to take the necessary steps to ensure that staff hired are aware of the Entity's information systems policies and adhere to them.

3.2 PURPOSE

The purpose of this policy is to ensure that partners, employees and third party contractors are aware of their responsibilities (including Information Security Policies) and are suitable for the roles for which they are considered. It also ensures that end-users are aware of information security threats and concerns, and are equipped to support MBA's information security policies in the course of their normal work.

This policy shall ensure the implementation of appropriate protection measures to minimise the risk of:

- Human error;
- Disclosure of confidential information; and
- Misuse of information assets.

This policy applies to all staff of MBA, including contract staff. All information assets of the Entity are also covered in this policy. The security responsibilities addressed here span the entire employment life cycle of an employee in MBA and shall be adhered to. MBA has selected different periods in an employment lifecycle in which the Human Resource Security Policy shall be adhered to by incoming employees, employees and outgoing employees.

3.3 POLICY

3.3.1 PRIOR TO EMPLOYMENT

3.3.1.1 SCREENING

All potential employees, or contract staff of MBA shall be subject to background checks, in line with local laws and regulations, and in accordance with the role being filled. This may include employment history (through character references and requests from terminated employments), educational credentials (through proof of academic and professional qualifications), medical checks, identity check and criminal record check. The level of screening/verification carried out for each role shall be commensurate to the business requirements for the role, the classification of information to be accessed by the role and the inherent risks

3.3.1.2 TERMS AND CONDITIONS OF EMPLOYMENT

Contractual agreements shall be made between MBA and its personnel and contractors. This will include an oath of confidentiality which must be signed before undertaking any

duties. The contracts shall expressly outline their information security responsibilities and shall specify the relationship between the employee and the employer. There shall be an inclusion in the agreement which will require the personnel/contractor to clearly state that he/she has read and understands the provisions of the terms and conditions.
There shall also be a mandatory information security awareness training at the point of induction, which will further explain what is expected of each personnel in terms of information security.

3.3.2 During Employment

3.3.2.1 Management Responsibilities

Management shall ensure that all staff and third-party personnel in MBA comply with the established Information Security policies and procedures. This shall be achieved through regular review and monitoring.

3.3.2.2 Information Security Awareness, Education And Training

The roles and responsibilities of end-users as regards Information Security shall be effectively communicated by ensuring that the policies are easily accessible on the intranet, and the link communicated. Additionally, there shall be mandatory periodic trainings held to ensure that the end-users are reminded of their responsibilities. Records of completion of training shall be maintained in line with the Entity’s retention policy.
Managers shall also monitor the work performance of their staff and hold periodic appraisals to identify training needs and to discover any problem areas, particularly where staff deal with sensitive information or work on sensitive computer applications.

3.3.2.3 Disciplinary Process

Any MBA personnel or third party who breaches the Entity’s Information Security policies shall be subject to disciplinary measures. These disciplinary measures shall be consistent with the severity of the action and may include, but are not limited to:

- Loss of access rights to data processing facilities
- Cancellation of contracts and eventual dismissal of consultants
- Termination of employment

3.3.3 Termination And Change of Employment

3.3.3.1 Termination or Change of Employment Responsibilities

MBA’s HR and ICT departments shall establish procedures for disengagement or change of employment responsibilities. Once an employee/contractor’s function has been modified in the organisation, he/she shall have their logical access rights modified in line with their new roles. Likewise for termination, after disengagement procedures have been duly followed, the personnel/contractor shall have his or her logical access to the Entity’s information assets revoked. In addition, all assets of the Entity in possession of the employee shall be returned and the Entity shall have proof of acknowledgement. Furthermore, information security responsibilities and duties that remain valid after the employee/contractor’s terminations shall be communicated to the employee/contractor and enforced.

4 Asset Management Policy

4.1 Introduction

Information assets are critical to processing of MBA's information. Therefore, it is essential that these information assets are documented, controlled and monitored, to ensure the most effective and efficient utilisation of resources. Information should also be classified to indicate the need, priorities and degree of protection required based on confidentiality, integrity and availability. This information classification system will define an appropriate set of protection level and special handling measures required for the degree of sensitivity and criticality of the asset.

4.2 Purpose

The purpose of this policy is to establish management and accountability for asset management and the implementation of appropriate measures to minimise the risk of:

- Data integrity, availability and confidentiality being compromised;
- Financial risks being incurred and/or;
- System performance being disrupted and/or degraded;
- Reputational damage and financial loss;
- Damage due to misuse, mischief or accident;
- Loss through theft or other fraudulent activity;
- Disruption of service due to theft; and
- Misconfiguration, as assets may not be properly labelled.

4.3 Policy

4.3.1 Responsibility for Assets

4.3.1.1 Inventory of Assets

All information assets of MBA shall be identified, and an inventory of such assets shall be drawn up and maintained. A detailed inventory containing descriptions of all critical information assets shall be documented and maintained. Documentation shall include:

- Information Custodian: Every critical information asset should be assigned an appropriate Information Custodian who is responsible for the information asset;
- Identification: Every critical information asset should be uniquely identified. The identification scheme used for this must ensure that:
  - ➢ The location of the information asset is known;
  - ➢ The supplier of the information asset is known (supplier information must be available);
  - ➢ Maintenance contract(s) for the information assets are identified.
- Description: a short description should be available for every information asset. The description should include general information on the information assets, such as its main function and use.

- Configuration: Technical configuration documentation should be included and supported by business requirements explaining why the information asset has been configured as such. This documentation should include licensing information.
- Major assets include manuals, software (applications, tools, and utilities) CDs, equipment and media.

A formal process shall be in place to capture critical information assets on the inventory register when purchased, deleted, sold or taken out of use. A physical account of these assets shall be taken at least once a year, and compared to the inventory listing of all assets for accuracy and completeness. There shall be backup of all information assets away from the primary location of the Entity.

4.3.1.2 OWNERSHIP OF ASSETS

It is the responsibility of all employees of MBA to ensure that all information assets of the Entiyty are adequately secured and accounted for. However, for the purpose of ownership, all physical and information assets belonging to MBA will have an identified, agreed and documented “owner” who will be responsible for the asset, its classification, use and management throughout its lifecycle.

4.3.1.3 ACCEPTABLE USE OF ASSETS

Information assets may only be used by all MBA employees including temporary staff, contractors, service providers and consultants and only for the purpose of performing the business of MBA. Information classified as highly confidential or confidential must not be made publicly available.The following should serve as guidelines for end users with regards to the acceptable use of Information Assets:

- Users shall not install any unauthorised software on Servers, PCs, laptops or any computing device belonging to MBA.
- Users shall not use the company facilities or assets for any form of unauthorised personal use.
- Mechanisms shall be put in place to monitor and control the installation of software on the entity’s Servers, PCs, and laptops.
- Any user requiring additional licensed software (to perform his/her job function) not in the list of approved software packages for the entity shall request the approval of the Head of Department and the Head, ICT before the software is installed.
- Users shall ensure that all use of software complies with the terms of the license.
- End users shall be responsible for safeguarding all personal computing equipment in their custody.
- Prior to disposal of media/asset (e.g. laptops, servers, flash drives, tapes) all information stored on the media must be carefully erased to prevent the possibility of recovery/reconstruction of the information.
- Documents containing confidential information must be disposed in a controlled manner (e.g. shredding) to guide against scavenging.

4.3.1.4 RETURN OF ASSETS

Each personnel, prior to departure from MBA (i.e upon employment/contract termination), is mandated to return all information assets belonging to MBA. There shall be proof of return of all assets, which shall be documented appropriately.

4.3.2 Information Classification

4.3.2.1 Classification of Information

Due to varying degrees of information sensitivity and citicality, MBA's information shall be classified according to legal requirements, value,criticality and sensitivity to unauthorised disclosure or modification. This classification system shall be used to define an appropriate set of controls and handling measures.

4.3.2.2 Labelling of Information

All MBA information assets shall be classified and labelled based on the value of their importance

To MBA. MBA will adopt the following classification methodology:

- Public (Published in any public forum without constraints either enforced by law or discretionary).
- Confidential (default classification) (Internal Information which may not be disclosed outside of MBA - represents a competitive advantage for the business).
- Highly Confidential (Only for use within specified segments in the organisation – Information for which unauthorised disclosure may give access to business secrets.).

All physical assets shall also be classified according to their level of importance and shall follow the following classification methodology:

- Critical – Physical assets which produce confidential (or secret) information and/or have a high value e.g. servers, routers, switches
- Standard – Physical assets which produce internal / public information and/or have a low value e.g. printers, stand-alone PCs.

4.3.2.3 Handling of Assets

Users shall be made aware of their responsibilities for securely handling classified information according to their classification. In addition, users shall be made aware of the necessary controls to implement for the various categories of information.

- Classification labels (physical) will be applied to classified information that are not processed by IT systems (e.g. manuals). Classified information and outputs from systems handling organisationally classified data will be labelled appropriately.
- Classification labels (physical or electronic) will be given to IT system outputs to reflect the classification of the most sensitive data in the output.

4.3.3 Media Handling

4.3.3.1 Management of Removable Media

All removable media of MBA must be encrypted, so as to secure information assets of the Entity stored therein. Information assets classified as 'Confidential' and 'Highly Confidential' shall not be stored on the removable media. End-users in possession of removable media used to store information assets have the responsibility of securing the media, and must report to the ICT department in the event of theft or loss of removable media.

4.3.3.2 Disposal of Media

Removable media shall be securely disposed of when no longer required for business. Periodic reviews shall be performed to ensure that stored data is in line with the data retention policy of MBA.

4.3.3.3 Physical Media Transfer

Media containing information assets of the Entity shall be secured against unauthorised access, misuse or corruption during transfer of files.