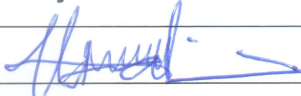


The Board and Management of the Nigeria Deposit Insurance Corporation considers Information Security as top priority in all areas of its operations, as this will ensure stakeholder confidence and protection of the Corporation's brand.

The Nigeria Deposit Insurance Corporation (NDIC) is committed to preserving the confidentiality, integrity, and availability of all information assets throughout the organization. Information and Information Security requirements will continue to be aligned with organizational goals and the NDIC's Information Security Management System (ISMS). The management system is intended to be an enabling mechanism for information sharing, electronic operations, e-commerce and reducing information-related risks to an acceptable level.

In pursuit of its primary objectives, the Corporation shall establish, implement, maintain and continually improve the ISMS designed to meet the requirements of ISO/IEC 27001:2013 and ensure that:

- i. NDIC's current strategic business plan and risk management framework provides the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an Information Security Management System (ISMS). The Risk Assessment report, Statement of Applicability and Risk Treatment Plan should identify how information-related risks are controlled. Enterprise Risk Management (ERM) is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments would, where necessary be carried out to determine appropriate controls for specific risks;
- ii. Information security continuity and contingency plans, data backup procedures, vulnerability management, access control to systems and information security incident reporting are fundamental to this policy
- iii. Control objectives from the ISMS perspective covering each of the areas as stated in the Statement of Applicability areas and they are further supported by specific documented policies and procedures;
- iv. All employees of NDIC and external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy;
- v. The ISMS is subject to continuous, systematic review and improvement. NDIC is committed to achieving certification of its ISMS to ISO27001: 2013. This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually;
- vi. NDIC has established a top-level Enterprise Risk Management team. IT Specific risk will be assessed to support the ISMS framework and to periodically review the performance of the management system and its various components;
- vii. The Corporation's Management, employees and any relevant external parties have been communicated and will continuously be informed regarding their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policies and procedures defined with respect to the ISMS) and to act in accordance with the requirements of the ISMS;
- viii. NDIC complies with applicable legal, regulatory, contractual and other requirements on Information Security;
- ix. All employees will receive information security awareness training and more specialised employees will receive appropriate specialized information security training.

Date	Signed By	Designation
18/8/22		EXECUTIVE DIRECTOR/OPS