OVERARCHING IMS POLICY (INFORMATION SECURITY AND BUSINESS CONTINUITY POLICY)

1. The Board and Management of Fincra located at the second floor of Polystar Building, Maruwa) which operates in the financial sector, provides excellent financial services and are committed to preserving the confidentiality, integrity, availability, and business continuity of all the physical, electronic information asset and customer information (this includes funds, account numbers, personally identifiable information, etc.) throughout the organization in order to preserve its competitive edge, assets, profitability, legal, regulatory as well as contractual, compliance and commercial image.

2. Information security and business continuity requirements will continue to be aligned with organizational goals and objectives, and the Information Security and Business Continuity Management System (ISMS & BCMS) is intended to be an enabling mechanism for information sharing, processing, transmitting, storage, electronic operations, e-commerce and reducing information-related risks to acceptable levels while also fortifying our ability to respond effectively to disruptions and safeguarding our stakeholders' trust and interests.

3. Fincra’s current strategy and Information Security and Business Continuity Management framework provide the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of IMS. The Information Security and Business Continuity Manager is responsible for the management and maintenance of the risk treatment plan.

4. In particular, business continuity and contingency plans, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. All employees of Fincra have the responsibility of reporting Security breaches.

5. All employees of Fincra and related external parties identified in the IMS are expected to comply with this policy. All staff will receive ISMS and BCMS related training and related external parties will be required to provide evidence of ISMS training.

6. Fincra has established an Information Security Forum (ISF) (or IT Steering Committee depending on which is used within the organization) with members drawn from across the organization.

7. Fincra is committed to aligning its processes, operations, products and services to the ISO27001:2022, ISO22301:2013, NDPR and PCIDSS requirements to ensure cyber resilience, integrated service management system and protection of its information assets.

8. The IMS is subject to continuous and systematic review with improvements, where necessary.

9. The IMS Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed and reapproved by the Board at least annually and also in the event of relevant changes and/or incidents.

10. A current version of this document is available to all members of staff on Confluence. It does contain confidential information and when considered not to be confidential can be released to relevant external parties.

11. This IMS policy was agreed to and approved by the Board and Executive Management and is issued on a version-controlled basis under the signature of the IMS Manager

12. Breach of this policy or any security mechanism may warrant disciplinary actions, up to and including termination of employment/contract.

Wole Ayodele	CEO		July 7th 2023