Central Bank of Nigeria
Payments System Policy Department
Central Business District,
Cadastral Zone,
P.M.B 0187, Abuja–Nigeria.
E-mail: PSPD@cbn.gov.ng
Phone :09 462 35000

PSP/DIR/PUB/CIR/001/004 **November 5, 2026**

CIRCULAR TO VIRTUAL ASSET SERVICE PROVIDERS IN NIGERIA AND STAKEHOLDERS IN THE FINANCIAL SERVICES INDUSTRY

REGULATIONS FOR THE OPERATIONS OF NON-SECURITY VIRTUAL ASSETS IN NIGERIA

To promote responsible innovation, strengthen the integrity of the Nigerian financial system and provide an appropriate regulatory framework for emerging digital payment instruments, the Central Bank of Nigeria (the Bank) hereby issues the attached **Regulations for the Operations of Non-Security Virtual Assets in Nigeria**.

1.0 Legal Basis

The Regulations are issued pursuant to the powers conferred on the Bank by:

- the Central Bank of Nigeria Act, 2007;
- the Banks and Other Financial Institutions Act, 2020; and
- other applicable laws.

The Regulations establish a comprehensive, risk-based framework for the licensing, authorisation, regulation, supervision and oversight of Non-Security Virtual Assets and related activities in Nigeria. They cover, among other matters, stablecoins, Deposit Money Tokens, Virtual Asset Service Providers, virtual asset payment services, platform-facilitated peer-to-peer services, custody, transfer, remittance, clearing and settlement activities.

2.0 Scope

The Regulations also prescribe requirements relating to:

a) Classification and designation of regulated tokens and activities;
b) Licensing and authorisation of issuers and providers of Non-Security Virtual Asset services;
c) Capital, reserve-backing, liquidity and redemption requirements;
d) Corporate governance, risk management and internal control systems;
e) Technology risk, cybersecurity and operational resilience;
f) Safeguarding of reserve assets and customer assets;
g) Customer protection, disclosures and complaints management;

h) Anti-money laundering, counter-terrorist financing and counter-proliferation financing obligations;
i) Sanctions screening, transaction monitoring and blockchain analytics;
j) Travel Rule compliance and counterparty VASP due diligence;
k) Regulatory reporting, supervisory access and information-sharing requirements; and
l) Enforcement, administrative sanctions and orderly wind-down arrangements.

The Regulations apply to persons carrying out regulated activities in or from Nigeria, directing such activities at persons in Nigeria, or undertaking activities that may materially affect the Nigerian payments system, financial system, foreign exchange market or financial stability. They may apply irrespective of whether the relevant person maintains a physical presence in Nigeria.

3.0 Regulatory Coordination

The Regulations do not displace the statutory mandate of the Securities and Exchange Commission or any other competent authority. Activities involving security virtual assets, securities, investment contracts or other capital-market products shall remain subject to the applicable capital-market regulatory framework. Where an activity involves both Non-Security Virtual Assets and matters falling within another authority's mandate, the relevant approvals shall be obtained from each competent authority.

All affected institutions, issuers, service providers, operators, promoters and other stakeholders are required to familiarise themselves with the Regulations and ensure full compliance with the applicable licensing, authorisation, prudential, operational, reporting, AML/CFT/CPF, customer-protection and technology requirements.

4.0 Commencement

The Regulations for the Operations of Non-Security Virtual Assets in Nigeria shall take effect from November 5, 2026.

Musa I. Jimoh
Director, Payments System Policy Department

Central Bank of Nigeria

REGULATIONS FOR THE OPERATIONS OF NON-SECURITY VIRTUAL ASSETS IN NIGERIA

TABLE OF CONTENTS

Part 1 — General Provisions 7
Introduction 8
Objectives 8
Scope 9
Legal Basis 10
Applicability 11
Exclusions 12
Principles of Interpretation 12

Part 2 — Definitions 14
Section 1 — Definitions 14

Part 3 — Prohibitions, Designation and Exemptions 22
Section 2 — Prohibitions on Activities and Promotions 22
Section 3 — Designation and Classification of Regulated Tokens and Activities 23
Section 4 — Delineation with the Securities and Exchange Commission 25
Section 5 — Exemptions 27

Part 4 — Licensing and Authorisation 29
Section 6 — Licence Categories 29
Section 7 — Issuer Licence Conditions and Application Requirements 30
Section 8 — Issuer Licensing Procedure and Approval-in-Principle 34
Section 9 — Licensing and Authorisation for Other Non-Security Virtual Asset Services 36
Section 10 — Platform-Facilitated Peer-to-Peer Services 43
Section 11 — Additional Requirements for Class 2 Stablecoins 50

Part 5 — Supervisory Powers 60
Section 12 — Authority Over Licensees 60
Section 13 — Restrictions on Regulated Tokens and Services 60
Section 14 — Suspension, Withdrawal and Revocation of Licences and Authorisations 61

Part 6 — Operational Requirements 65
Section 15 — Capital Requirements for Class 1 and Class 2 Licensed Issuers 65
Section 16 — Capital Requirements for Other Non-Security Virtual Asset Services 65
Section 17 — Supplementary Capital, Liquidity and Systemic Requirements 66

Section 18 — Assessment of Shareholders, Controllers, Directors and Senior Management ... 67
Section 19 — Principal Business ... 70
Section 20 — Notification, Reporting and Annual Compliance Requirements ... 71
Section 21 — Use of Agents and Distributors ... 73
Section 22 — Outsourcing ... 74
Section 23 — Issuance and Redemption of Stablecoins ... 74
Section 24 — Management and Safekeeping of the Reserve Pool ... 76
Section 25 — Safeguarding Tokens and Customer Assets Held for Custody and Transfer ... 89

Part 7 — AML/CFT/CPF Obligations ... 91

Section 26 — Anti-Money Laundering, Counter-Terrorist Financing, Counter-Proliferation Financing and Sanctions ... 91

Part 8 — Customer Protection and Conduct ... 112

Section 27 — Obligations Towards Customers and Complaints ... 112
Section 28 — Stablecoin Whitepapers ... 113
Section 29 — Customer Agreements ... 114
Section 30 — Required Terms and Pre-Contractual Information ... 114
Section 31 — Transactional Information ... 115
Section 32 — Protection of Payment and Personal Data ... 115
Section 33 — Unauthorised Transfers, Errors, Liability and Refunds ... 115
Section 34 — Certainty and Finality of Transfers ... 116

Part 9 — Governance, Risk and Technology ... 118

Section 35 — Corporate Governance ... 118
Section 36 — General Risk Management and Internal Control Systems ... 118
Section 37 — Technology Risk and Information Security ... 120
Section 38 — Business Continuity, Recovery and Orderly Wind-Down ... 123

Part 10 — Deposit Money Tokens ... 127

Section 39 — Definition of Deposit Money Tokens ... 127
Section 40 — Legal Status and Deposit Treatment ... 127
Section 41 — Eligibility and Approval to Issue Deposit Money Tokens ... 127
Section 42 — Issuance, Backing and Redemption ... 127
Section 43 — Transfer and Settlement ... 128
Section 44 — Wallets, Custody and Third-Party Participation ... 129
Section 45 — Permitted Uses and Programmability ... 129

Section 46 — Risk Management, AML and Customer Protection 129
Section 47 — Reporting and Supervisory Requirements 130
Section 48 — Cross-Border Transactions 131
Section 49 — Regulatory Pilot Arrangements 131
Section 50 — DMT Supervision and Enforcement 131

Part 11 — Enforcement and Final Provisions 133

Section 51 — Enforcement and Administrative Sanctions 133
Section 52 — Additional Information-Gathering and Cooperation Powers 134
Section 53 — Relationship with Other Regulatory Frameworks 137
Section 54 — Transition and Pilot Arrangements 137
Section 55 — Interpretation 137
Section 56 — Publication, Commencement and Application 138

Schedules

Schedule 1 — Licence and Authorisation Application Letter 140
Schedule 2 — Fit and Proper Questionnaire 143
Schedule 3 — Fee Schedule 144
Schedule 4 — CBN Reserve Deposit Account Agreement: Prescribed Terms 145
Schedule 5 — Stablecoin Whitepaper Requirements 146
Schedule 6 — Reserve Attestation Report Format 147
Schedule 7 — Supervisory Reporting Templates 149
Schedule 8 — CBN and SEC Delineation Matrix 157

Annex

Documents to Be Submitted with an Application 161

Part 1
General Provisions

Introduction

The emergence of virtual assets, stablecoins, and tokenised payment instruments presents significant opportunities for innovation in payments, remittances, settlement, and digital commerce. However, their growing adoption also introduces risks relating to financial stability, monetary policy, consumer protection, illicit finance, operational resilience, and foreign exchange management.

Pursuant to its statutory mandate to promote monetary and financial stability and regulate Nigeria's payments system, the Central Bank of Nigeria (CBN) issues these Regulatory Guidelines for the operations of Non-Security Virtual Assets in Nigeria. These Guidelines establish a risk-based framework for the licensing, regulation, supervision, and oversight of Non-Security Virtual Assets, including stablecoins, Deposit Money Tokens (DMTs), and related Virtual Asset Service Providers (VASPs).

These Guidelines seek to support responsible innovation while safeguarding the integrity, stability, and efficiency of the Nigerian financial system. These Guidelines also seek to provide regulatory requirements relating to governance, prudential standards, consumer protection, operational resilience, AML/CFT/CPF compliance, and reporting obligations for entities and persons engaged in regulated non-security virtual asset activities within or involving Nigeria.

Nothing in these Guidelines shall be construed as extending their requirements to virtual assets that constitute securities, investment contracts, or other capital market products falling within the statutory jurisdiction of the Securities and Exchange Commission (SEC). The CBN shall, where necessary, collaborate with other competent authorities to ensure effective oversight of the virtual asset ecosystem. Where an activity falls within the concurrent jurisdiction of another competent authority, such activity shall be regulated in accordance with applicable inter-agency coordination arrangements.

Objectives

The objectives of these Guidelines are to:

a) establish a comprehensive, risk-based regulatory framework governing the issuance, distribution, conversion, custody, transfer, redemption and settlement of Non-Security Virtual Assets, including stablecoins and Deposit Money Tokens;

b) preserve the effectiveness of the Bank’s monetary policy instruments and its capacity to monitor and manage capital flows and foreign exchange dynamics;

c) protect holders and consumers from issuer insolvency, reserve or backing mismanagement, redemption denial, fraud and other conduct risks;

d) safeguard the stability and integrity of the Nigerian financial system;

e) support safe innovation and the integration of virtual assets into Nigeria’s digital payments and settlement infrastructure in a manner consistent with applicable laws and the Bank’s mandate;

f) provide guidance on licensing requirements and ongoing compliance obligations for persons conducting regulated activities;

g) enable the effective implementation and enforcement of AML/CFT/CPF requirements; and

h) provide guidance on customer due diligence, customer identification and verification, Travel Rule and related compliance requirements applicable to virtual asset service providers.

Scope

I. These Guidelines establish the requirements for the licensing, authorisation, regulation and supervision of the following Regulated Activities, when carried out in or from Nigeria, directed at persons in Nigeria, or otherwise falling within the jurisdictional scope of these Guidelines:

a) issuance, offering and distribution;

b) market access, intermediation and agency services;

c) exchange or conversion, including:

i) exchange between Regulated Tokens and fiat currency; and

ii) exchange between one or more forms of virtual assets;

d) fiat on-ramp and off-ramp services;

e) custody, safekeeping and administration, including the provision of digital wallets and key management services;

f) transfer, payment, payment gateway and merchant-acceptance, stored-value, remittance, clearing and settlement services

g) operation of payments system infrastructure or settlement infrastructure;

h) reserve asset custody and related support services; and

i) any other activity as may be designated by the Bank.

II. These Guidelines apply to the following virtual assets and tokens (collectively, Regulated Tokens):

a) Naira-Referenced Stablecoins (Class 1);

b) Foreign Currency-Referenced Stablecoins (Class 2);

c) Deposit Money Tokens (DMTs);

d) Other Designated Tokens determined by the Bank to fall within its mandate over payments, settlement, foreign exchange, banking or financial stability; and

d) any other token designated by the Bank as a Regulated Token under these Guidelines.

III. The Bank shall determine whether a token, arrangement, service or activity falls within these Guidelines by reference to its economic substance, function and risk characteristics, rather than its name, legal form, marketing description or underlying technology.

Legal Basis

I. These Guidelines are issued by the Central Bank of Nigeria pursuant to:

a) the Central Bank of Nigeria Act, 2007, including its provisions relating to the promotion and regulation of payment systems;

b) the Banks and Other Financial Institutions Act, 2020;

c) the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act 1995;

d) the Money Laundering (Prevention and Prohibition) Act, 2022;

e) the Terrorism (Prevention and Prohibition) Act, 2022; and

f) all other applicable laws and regulations.

II. These Guidelines are issued in accordance with the Presidential Executive Order on Virtual Assets Coordination, 2026.

III. These Guidelines shall be read together with all applicable laws, regulations, guidelines and directives relating to:

a) banking;

b) payments system;

c) foreign exchange;

d) consumer protection;

e) data protection and privacy;

f) anti-money laundering;

g) counter-terrorist financing;

h) counter-proliferation financing; and

i) any other applicable legal or regulatory requirement.

IV. Nothing in these Guidelines displaces or limits the statutory mandate of another competent authority. Activities involving securities or other products that fall within the jurisdiction of another authority remain subject to the requirements of that authority. The Bank regulates only those aspects falling within its lawful mandate and may coordinate supervisory arrangements where appropriate.

Applicability

I. These Guidelines apply where:

a) a Regulated Activity is carried out in Nigeria;

b) a Regulated Activity is carried out from Nigeria;

c) a Regulated Activity is directed at persons in Nigeria;

d) a Regulated Token is offered, marketed, distributed or otherwise made available to persons in Nigeria; or

f) a Regulated Activity has, or is reasonably likely to have, a material effect on the Nigerian payments system, financial system, foreign exchange market or financial stability.

II. These Guidelines apply to any person performing a Regulated Activity, whether or not that person maintains a physical presence in Nigeria, including:

a) issuers;

b) foreign issuers whose Regulated Tokens are offered, marketed, distributed or made available to persons in Nigeria;

c) distributors and market access providers;

d) exchanges, conversion providers and trading platforms;

e) wallet service providers;

f) custodians and reserve asset custodians;

g) payment, payment gateway, merchant-acquiring, stored-value, remittance, clearing and settlement service providers;

h) payment system infrastructure providers;

i) agents and intermediaries; and

j) any other person performing a Regulated Activity under these Guidelines.

III. An overseas location does not remove an activity directed at Nigerian persons from the scope of these Guidelines. Every issuer whose token is admitted to the Nigerian market shall comply with the applicable incorporation, licensing and authorisation requirements prescribed under these Guidelines.

Exclusions

I. These Guidelines do not apply to:

a) any Central Bank Digital Currency issued directly by the Bank or any other jurisdiction;

b) Security Virtual Assets and other securities, investment products and collective investment schemes, including their tokenised forms, which are subject to the Investments and Securities Act and regulated by the Securities and Exchange Commission; provided that any payment, settlement, foreign exchange or other activity falling within the mandate of the Bank remains subject to these Guidelines in respect of that activity;

c) electronic money, stored-value products and their tokenised forms regulated under applicable payments system laws and regulations, unless the Bank determines that a change in functionality requires authorisation under these Guidelines;

d) bank liabilities that do not constitute deposits and are not Deposit Money Tokens;

e) loyalty points, rewards programmes, vouchers or similar instruments that may be used only within a limited network and cannot be exchanged for money or transferred to third parties;

f) any token or activity specifically exempted by the Bank; and

g) such other products, arrangements or activities as the Bank may designate.

Principles of Interpretation

a) These Guidelines shall be interpreted in a manner consistent with the statutory objectives and mandate of the Bank.

b) The categorisation, characterisation or description of a token, product, arrangement or service by any person is not determinative of its regulatory treatment under these Guidelines

c) The Bank may determine the regulatory treatment of any token, product, arrangement or activity according to its economic substance, functional characteristics, risk profile and potential impact on the Nigerian financial system, payments system, foreign exchange market or financial stability.

d) References to Regulated Tokens, Regulated Activities, issuers, service providers and other defined terms shall have the meanings assigned to them in Section 1 (Definitions).

e) Unless otherwise stated, references to any law, regulation, guideline or directive include any amendment, replacement or successor instrument.

Part 2
Definitions

Section 1 Definitions

In these Guidelines, unless the context otherwise requires, the following definitions apply.

Algorithmic Stablecoin, a purported stablecoin that relies solely or primarily on algorithmic mechanisms, including supply expansion or contraction protocols, to maintain price stability without the backing of commensurate reserve assets denominated in or equivalent to the reference asset.

AML/CTF/CPF, Anti Money Laundering, Counter Terrorist Financing and Counter Proliferation Financing

Approval to Extend Permitted Activities (AEPA), the written approval granted by the Bank under Sections 6.2(e) and 9.4A to a financial institution licensed by the Bank, extending the activities permitted under its Principal Licence to one or more specified Non-Security Virtual Asset Payment Activities.

Approval-in-Principle (AIP), the conditional preliminary approval under Section 8.5; it is not a final licence or authority to commence a Regulated Activity.

Approved Independent Auditor, a firm of chartered accountants registered with the Financial Reporting Council of Nigeria and approved by the Bank to conduct reserve attestations or audits required under these Guidelines.

Approved Virtual Asset Payment Instrument, a Regulated Token that has been approved or recognised by the Bank for use in a Non-Security Virtual Asset Payment Activity, whether by Token Approval, by approval under Part 10 or by a designation notice under Section 3.11. It does not include fiat currency, a deposit balance maintained in conventional form with a deposit-taking institution, electronic money, a payment account, a payment card, a payment token or other instrument regulated solely under the applicable payments framework, or any other digital payment instrument that is not a virtual asset.

Authorisation, an Other Services Authorisation or an Approval to Extend Permitted Activities, as the context requires, being express written permission granted by the Bank under Section 9 to provide specified Other Non-Security Virtual Asset Services.

Authorised Entity, the holder of an Other Services Authorisation or an Approval to Extend Permitted Activities granted under Section 9. References to a licensed or authorised VASP include a VASP holding the relevant CBN approval for the activity in question.

Bank, is the Central Bank of Nigeria.

BOFIA, is the Banks and Other Financial Institutions Act, 2020, as amended

Business Day, a day other than a Saturday, Sunday or public holiday declared by the Federal Government of Nigeria.

Customer Due Diligence (CDD), procedures undertaken to identify and verify a customer's identity, understand the nature and purpose of the business relationship, assess the customer's risk profile, and conduct ongoing monitoring to detect and report suspicious activities and ensure compliance with applicable regulatory requirements.

Chief Compliance Officer (CCO), means the senior officer designated under Section 26.2.2 as responsible for overseeing a Licensee's compliance with these Guidelines and applicable law, who shall also be the money laundering reporting officer for the purposes of the Money Laundering (Prevention and Prohibition) Act, 2022.

Chief Executive Officer (CEO), the principal executive officer of an issuer or regulated institution, by whatever title designated

Chief Risk Officer (CRO), the senior officer responsible for identifying, assessing and managing the material risks arising from an issuer's or regulated institution's operations.

Class 1 Stablecoin, a Naira-Referenced Stablecoin that has received Token Approval and is issued by a Class 1 Licensed Issuer.

Class 2 Stablecoin, a Foreign-Currency-Referenced Stablecoin that has received Token Approval and is issued by a Class 2 Licensed Issuer.

Control, the ability, whether alone or jointly with another person, to initiate, authorise, block, reverse or otherwise effect a transaction involving a Regulated Token or other virtual asset held for a customer, including through the use of private keys, seed phrases, signing infrastructure or other access credentials

Council, the Virtual Asset Council established under the Presidential Executive Order on Virtual Assets Coordination, 2026 to coordinate the regulation of virtual assets and determine questions of classification and jurisdiction between the Bank and the SEC.

Custodial Virtual Asset Payment Wallet, a wallet or arrangement under which a person, for or on behalf of a customer, holds, safeguards or administers an Approved Virtual Asset Payment Instrument, private key or other means of access, or otherwise has Control of the Approved Virtual Asset Payment Instrument, including the ability to initiate or authorise its transfer.

Custodian, a person approved or licensed, where required by the Bank, to hold or safeguard reserve assets, tokens, private keys or other instruments enabling control over tokens on behalf of an issuer or customer.

Customer Agreement, the written terms governing the regulated service and the rights and responsibilities of the customer and provider.

Deposit Money Bank (DMB), a bank licensed by the Bank to carry on deposit-taking banking business in Nigeria.

Deposit Money Token (DMT), means a digital token issued by a Deposit Money Bank that represents a direct claim on that Issuing Bank and corresponds to an existing deposit liability denominated in Naira.

Eligible Reserve Assets, assets permitted under these Guidelines to be held in a Reserve Pool to back Stablecoins in circulation.

The Financial Action Task Force (FATF), the intergovernmental body that sets international standards for anti-money laundering, counter-terrorist financing, and counter-proliferation financing.

Foreign Currency Issuer Licence (Class 2), the licence granted by the Bank under Section 6.2(b) authorising the issuance of Class 2 Stablecoins.

Foreign Currency-Referenced Stablecoin, a Stablecoin designed to maintain a stable value by reference to a currency other than the Naira.

High-Quality Liquid Assets (HQLA), Eligible Reserve Assets that can be readily converted into cash with minimal or no loss of value and meet the liquidity criteria prescribed or adopted by the Bank. Assets counted towards Section 24.12 shall satisfy its maturity requirements and applicable category-specific limits; asset eligibility under Section 24.28 alone shall not establish HQLA status.

Issuer Licence, a Naira-referenced Issuer Licence (Class 1) or a Foreign Currency Issuer Licence (Class 2).

Issuing Bank, the Deposit Money Bank that issues a DMT and remains liable for the underlying deposit claim represented by that DMT.

Know Your Customer (KYC), the process by which a regulated entity verifies the identity of its customers and assesses the risk of money laundering, terrorist financing, and proliferation financing associated with those customers.

Licensed Issuer, a Nigerian incorporated entity holding an Issuer Licence. "Class 1 Licensed Issuer" means the holder of a Naira-referenced Issuer Licence (Class 1), and "Class 2 Licensed Issuer" means the holder of a Foreign Currency Issuer Licence (Class 2). A reference to a "Licensed Stablecoin Issuer" is a reference to a Licensed Issuer.

Licensee, a Licensed Issuer, the holder of an Other Services Licence, the holder of an Other Services Authorisation or the holder of an Approval to Extend Permitted Activities. References to a licensed or authorised VASP include a VASP holding the relevant licence or authorisation from the Bank for the activity in question.

Minting, the process of creating new stablecoin tokens by a Licensed Issuer upon receipt of equivalent reserve assets.

MLPPA, Money Laundering (Prevention and Prohibition) Act, 2022

Naira (NGN), the lawful currency of the Federal Republic of Nigeria.

Naira-referenced Issuer Licence (Class 1), the licence granted by the Bank under Section 6.2(a) authorising the issuance of Class 1 Stablecoins.

Naira-Referenced Stablecoin, a Stablecoin designed to maintain a stable value by reference to the Naira on a one-to-one basis and backed by Naira-denominated Eligible Reserve Assets.

NDIC, the Nigeria Deposit Insurance Corporation.

NFIU, the Nigerian Financial Intelligence Unit.

Non-Security Virtual Asset, virtual asset that is not a Security Virtual Asset and that is designed, used or intended primarily as a means of payment, settlement or transfer of value, or as a unit of value held for such purposes, and includes a stablecoin, a Deposit Money Token and an Other Designated Token.

Non-Custodial Virtual Asset Payment Wallet, a wallet or arrangement that enables a customer to hold, access, receive, transfer, redeem or otherwise manage an Approved Virtual Asset Payment Instrument, where the customer retains sole Control of the private keys or other means of accessing and controlling the Approved Virtual Asset Payment Instrument and the wallet provider cannot independently transfer or otherwise exercise Control over it.

Non-Security Virtual Asset Payment Activity, any activity involving an Approved Virtual Asset Payment Instrument that falls within the regulatory mandate of the Bank, including any of the following: (a) the provision or operation of a Custodial Virtual Asset Payment Wallet; (b) the facilitation, processing, routing, clearing, settlement or reconciliation of payments; (c) a Virtual Asset Payment Gateway Service, including merchant-acquiring or payment-acceptance services; (d) domestic or cross-border transfer services; (e) remittance services; (f) the operation of a Virtual Asset Stored-Value Facility; (g) the operation or facilitation of a Platform-Facilitated Peer-to-Peer Service involving exchange or conversion against Naira, payment, transfer or settlement functionality, in accordance with Section 10; and (h) any other payment, transfer, remittance, clearing, settlement or stored-value activity designated by the Bank.

Operational Liquidity, readily accessible liquidity maintained by a Class 2 Licensed Issuer under Sections 11 and 24.50 to meet expected and stressed Nigerian redemption and payment obligations, and which is separate and does not replace the Reserve Pool and required capital.

Other Designated Token, a Non-Security Virtual Asset designated by the Bank under Section 3 and not otherwise classified under these Regulations.

Other Non-Security Virtual Asset Services, the non-issuance services described in Section 9, including Non-Security Virtual Asset Payment Activities.

Other Services Authorisation, the written authorisation granted by the Bank under Sections 6.2(d) and 9 to a person holding a SEC licence for securities-related virtual asset services, permitting it to provide specified Other Non-Security Virtual Asset Services.

Other Services Licence, the Other Non-Security Virtual Asset Services Licence granted by the Bank under Section 6.2(c) to a person that does not hold a SEC licence.

Person of Significant Control, a person who exercises direct or indirect control over an entity, through ownership, voting rights, agreement or other means.

Platform Facilitated Peer-to-Peer Service (P2P), a service through which a person facilitates transactions between customers for the purchase, sale or exchange of a Regulated Token against Naira or another permitted form of value, including by providing matching, order display, escrow, payment facilitation, settlement support, transaction verification or dispute resolution. A P2P Service does not include a purely private bilateral transfer in which no person other than the transacting parties operates, facilitates, intermediates or supports the transaction.

Principal Licence, a valid licence issued by the CBN under which a financial institution carries on its principal regulated business, including deposit-taking, electronic money, mobile money, payment services, transfer, international money transfer, switching, clearing or settlement, and which may form the basis of an Approval to Extend Permitted Activities under Section 9.6.

Prohibited Token, a token within any of the categories listed in Section 2.2, the issuance, offer, distribution, trading or availability of which to persons in Nigeria is prohibited under these Regulations.

Redemption, the process by which a holder presents tokens to the Licensed Issuer, or to a Licensee acting on its behalf, and receives the corresponding fiat currency or value, or by which a DMT is converted or paid out against the underlying deposit liability, as applicable.

Regulated Activity, an activity within the scope of these Regulations and the Bank's statutory mandate, including issuance, distribution, exchange, conversion, custody, wallet, transfer, payment, payment gateway, merchant-acceptance, stored-value, remittance, clearing and settlement services, or another activity designated under Section 3.

Regulated Token, a Class 1 Stablecoin, a Class 2 Stablecoin, a Deposit Money Token or an Other Designated Token.

Regulations, the Regulations the Operations of Non-Security Virtual Assets in Nigeria.

Reserve Attestation, a report prepared by an Approved Independent Auditor confirming, within the stated scope and reference date, the composition, value, coverage and segregation of a Licensed Issuer's reserve assets.

Reserve Deposit Account, the account maintained at the Bank by a Class 1 Licensed Issuer under Section 24.25 and Schedule 4.

Reserve Pool, the aggregate Eligible Reserve Assets maintained by a Licensed Issuer to back its Stablecoins in circulation.

RTGS, Real Time Gross Settlement System.

SEC, The Securities and Exchange Commission of Nigeria.

Security Virtual Asset, a virtual asset that; (a) represents or confers rights equivalent to a share, debenture, bond, unit in a collective investment scheme, derivative or other security within the meaning of the Investments and Securities Act, 2025; (b) is offered, marketed or held on terms that give rise to a reasonable expectation of profit, return or yield derived wholly or mainly from the efforts of the issuer, a promoter or a third party, including an investment contract; or (c) has been determined to be a security by the SEC or, in a case of dispute, by the Council; but does not include a Regulated Token issued or approved under these Regulations which confers on its holder no right other than a right of redemption at par in the reference currency and no interest, return or other financial benefit.

Settlement Infrastructure, a payment, clearing or settlement system approved or designated by the Bank for the settlement of transactions, including interbank DMT transactions.

Significant Shareholder, a person holding five per cent or more of issued share capital.

Smart Contract, a self-executing programme deployed on a blockchain network that automatically executes predefined operations, including minting, burning, freezing, and transferring stablecoin tokens, upon the occurrence of specified conditions.

Special Purpose Administrator, a person appointed by the Bank under Section 14.8 or 24.48.

Stablecoin, a cryptographic virtual asset designed to maintain a stable value relative to a specified reference asset, including a fiat currency, through reserve backing, collateralisation, or other stability mechanisms, and issued by or under the authority of a private entity.

Stress Event, an event or circumstance that has occurred or is reasonably likely to occur and that materially impairs, or threatens to impair, the ability of a Licensed Issuer to maintain reserve backing, provide timely redemption, safeguard Reserve Assets or continue critical issuance and redemption operations.

Systemic Stablecoin, a Stablecoin designated by the Bank under Section 3.6 or 3.7 as posing or potentially posing material systemic risk by reason of its scale, interconnectedness or criticality to payment or financial-market infrastructure.

Token Approval, the Bank's written approval of a specific token under Sections 7.4 and 8, covering its class, reference currency, reserve arrangements, name, ticker symbol and blockchain networks. Token Approval does not imply a guarantee by the Bank.

Travel Rule, the requirement, under FATF Recommendation 16 as applied to virtual asset transfers by Recommendation 15 and as revised from time to time, for virtual asset service providers and financial institutions to obtain, hold and transmit prescribed originator and beneficiary information alongside qualifying transfers.

TPPA, Terrorism (Prevention and Prohibition) Act, 2022

Unhosted Wallet, a virtual asset wallet or address in respect of which no Licensee, VASP, financial institution or other regulated intermediary holds, administers or exercises Control over the virtual assets, private keys or other means of access on behalf of the owner or user.

Virtual Asset Service Provider (VASP), being any natural or legal person that, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and participation in and provision of financial services related to an issuer's offer or sale of a virtual asset.

Virtual Asset, a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes, but does not include (a) digital representations of fiat currency, including Central Bank Digital currency and deposits recorded in conventional form, or (b) securities and other financial assets that are regulated as such under any other law, save that a Deposit Money Token shall be treated as a virtual asset for the purposes of Part 7 and Part 10.

Virtual Asset Payment Gateway Service, a service that facilitates the initiation, transmission, routing, processing, acceptance, reconciliation or settlement of a payment involving an Approved Virtual Asset Payment Instrument between an originator, beneficiary, merchant or payment service provider.

Virtual Asset Stored-Value Facility, a facility under which a person holds Approved Virtual Asset Payment Instruments on behalf of customers to enable them to make future payments or transfers, including a prepaid or stored-value account denominated in, or redeemable for, an Approved Virtual Asset Payment Instrument.

Wallet, means an application, device, account or other arrangement used to hold, store, send or receive tokens or to manage the credentials that enable control over them.

Whitepaper, the pre-issuance disclosure document required under these Regulations and Schedule 5.

Part 3
Prohibitions Designation and Exemptions

Section 2 Prohibitions on Activities and Promotions

2.1 Restrictions on Activities

2.1.1 No person shall conduct, or hold itself out as authorised to conduct, a Regulated Activity without the licence, authorisation or approval required by these Regulations. The licences and authorisations available under these Regulations are the

a) Naira-referenced Issuer Licence (Class 1);

b) Foreign Currency Issuer Licence (Class 2);

c) Other Services Licence;

d) Other Services Authorisation;

e) Approval to Extend Permitted Activities; and

f) Deposit Money Token Licence

2.2 The following categories of token are Prohibited Tokens and shall not be issued, offered, distributed or traded in Nigeria:

a) Algorithmic Stablecoins, being tokens that seek to maintain a stable value solely or primarily through algorithmic adjustment of supply or demand rather than full backing by Eligible Reserve Assets;

b) tokens that reference a fiat currency but are backed wholly or primarily by other virtual assets;

c) tokens issued by, or on behalf of, a sanctioned person or a person located in a sanctioned jurisdiction;

d) tokens that are represented or marketed as stablecoins but do not confer on their holders an enforceable right of redemption at par; and

e) any other token that the Bank determines, poses an unacceptable risk to monetary or financial stability, financial integrity or consumers.

2.3 Any person that issues, offers, distributes or facilitates access to a Prohibited Token in Nigeria shall be subject to the enforcement and administrative measures provided in Part 11 of these Regulations.

2.4 Lending or borrowing of Regulated Tokens requires separate approval under applicable law, and a licence, authorisation or Token Approval under these Regulations. shall not by itself authorise that activity. No lending, investment or other activity shall misuse customer assets or the Reserve Pool of a Licensed Issuer.

2.5 Restrictions on Promotions

2.5.1 No person shall promote a Regulated Activity for which the required licence, authorisation or approval has not been granted, or a Prohibited Token, misstate its licensing status, or use another person to circumvent a restriction under these Regulations. Advertising and promotion shall be fair, clear and not misleading and shall accurately identify the responsible Licensee and the applicable risks.

2.6 A licence, authorisation, Token Approval or capital deposit shall not be represented as an endorsement or guarantee by the Bank.

2.7 Class 1 Stablecoins and Class 2 Stablecoins shall not be represented as bank deposits or as covered by NDIC deposit insurance.

Section 3 Designation and Classification of Regulated Tokens and Activities

3.1 The Bank may designate a Non-Security Virtual Asset or related service within its statutory mandate for the purposes of these Regulations. A designation shall identify the token or activity, its scope, reasons and applicable requirements and shall be communicated by written notice, circular, guideline or directive. Designation shall not itself grant a licence, authorisation or Token Approval, or displace another authority's statutory mandate.

3.2 For the purposes of these Regulations, all stablecoins operating in, offered in, distributed in, or otherwise made available to persons in Nigeria shall be classified into the following categories:

a) Class 1 Stablecoins, being Naira-Referenced Stablecoins;

b) Class 2 Stablecoins, being Foreign-Currency-Referenced Stablecoins; and

c) Prohibited Tokens, being stablecoins within any of the categories listed in Section 2.2

d) Other Services Authorisation;

3.3 The classification of a stablecoin as a Class 1 Stablecoin, a Class 2 Stablecoin or a Prohibited Token shall be determined by the Bank having regard to the reference asset, the issuance architecture, the reserve structure and the primary use case of the instrument.

3.4 The licence categories applicable to each class of Regulated Token, and the rule on holding both Issuer Licences, are set out in Section 6.

3.5 Upon Token Approval, a stablecoin shall be designated a Class 1 Stablecoin or a Class 2 Stablecoin, as the case may be.

3.6 The Bank may, by notice in writing to the Licensed Issuer and to any Licensee acting as its distribution partner, designate a Class 1 Stablecoin or a Class 2 Stablecoin as a Systemic Stablecoin where, having regard to the circumstances of the Nigerian market, the Bank considers that enhanced supervisory requirements are warranted. A stablecoin shall be designated as a Systemic Stablecoin where:

a) the naira-equivalent value of its circulating supply exceeds five hundred billion naira (₦500,000,000,000.00) on each day for thirty consecutive days; or

b) it is held or used by more than five million (5,000,000) persons in Nigeria, as determined by the Bank on the basis of supervisory data.

3.7 Separately, the Bank may, at its discretion, designate a Class 1 Stablecoin or a Class 2 Stablecoin as a Systemic Stablecoin based on the following indicators:

a) circulating supply or Nigeria-linked value;

b) transaction volume and value;

c) number and concentration of Nigerian users or wallet addresses; and

c) the proportion of a stablecoin's activity attributed to the Nigerian market.

3.8 A Class 1 Stablecoin shall reference the Naira one-to-one, be fully backed by Naira-denominated Eligible Reserve Assets and be issued by a Class 1 Licensed Issuer. Approved uses may include payments, settlement, treasury management and the holding of balances incidental to such uses, subject to these Regulations, including the prohibition on interest and yield in Section 13.3.

3.9 A Class 2 Stablecoin shall reference a currency other than the Naira, and shall be issued by a Class 2 Licensed Issuer. Lawful uses include cross-border payments and remittances, trading through Licensees, international commerce and trade settlement, and holding or transferring foreign-currency value subject to applicable requirements.

3.10 The use of Class 2 Stablecoins for domestic Naira obligations and conversion against Naira shall remain subject to Sections 7.5, 11.7 and 13.2 and to applicable foreign-exchange regulations. Designation as a Systemic Stablecoin shall trigger the enhanced requirements in Section 17.

3.11 The Bank may designate a Non-Security Virtual Asset as an Other Designated Token by written notice where it considers, having regard to the token's economic function and primary use, that the token falls within the Bank's mandate over payments, settlement, foreign exchange, banking or financial stability.

a) The notice shall state the basis for the designation by reference to that mandate, name the Regulated Activities that require a licence or authorisation under Part 4, and exclude securities and investment products.

b) The Bank shall consult affected persons before a designation of general application. It may designate a token for one person without consultation where necessary to supervise that person.

c) A designation takes effect on the date in the notice. It is not retrospective.

d) Where there is a reasonable question whether the token is a Security Virtual Asset, the Bank shall refer the matter to SEC under Section 4.5 and, failing agreement within thirty Business Days, to the Council, and shall not designate the token pending that determination except on an interim basis to protect consumers or financial stability.

3.12 The exclusion of an asset from the scope of these Regulations shall not be construed as excluding any underlying activity from the regulatory oversight of the Bank. Any person undertaking a payment, settlement, banking, foreign exchange, custody, or other Regulated Activity through, by means of, or in connection with an excluded product shall continue to be subject to all applicable laws, regulations, licensing requirements, authorisations, directives, and supervisory obligations administered by the Bank.

Section 4 Delineation with the Securities and Exchange Commission

4.1 **Allocation Principle:** The allocation of regulatory responsibility under these Regulations follows the nature of the instrument and of the activity. The Bank regulates Non-Security Virtual Assets and the payment, settlement, money and value transfer, remittance, foreign-exchange, deposit-taking, lending and custody services provided in relation to them. The SEC regulates Security Virtual Assets and the capital market activities conducted in relation to them.

4.2 **Security Virtual Assets:** Nothing in these Regulations authorises any person to issue, offer, trade, advise on, manage or hold in custody a Security Virtual Asset, and no licence or authorisation granted by the Bank shall be represented as such authority.

4.3 **Activities Spanning both Mandates:** Where a person carries on activities within the mandates of both the Bank and SEC, it shall obtain the licence or authorisation required by each authority for the relevant activity. The authority responsible for the predominant activity shall act as lead supervisor, and the Bank and SEC shall coordinate the assessment of the application under Sections 9.3.1 to 9.3.3.

4.4 **Payment and Settlement Leg:** Where a Security Virtual Asset transaction is settled in naira, in foreign currency or in a Regulated Token, the settlement and payment services shall be subject to these Regulations to the extent they fall within the Bank's mandate, and the Security Virtual Asset shall remain subject to SEC.

4.5 **Classification:** A person who is uncertain whether a virtual asset constitutes a Security Virtual Asset or a Non-Security Virtual Asset shall, before issuing, offering, providing, facilitating or otherwise dealing in the virtual asset in Nigeria, apply to the Bank for a classification opinion. The Bank shall, where the classification of the virtual asset may fall within the regulatory jurisdiction of SEC, consult that authority before issuing its classification opinion.

4.6 **Cooperation:** The Bank and the SEC shall exchange supervisory information, notify each other of licensing decisions, enforcement actions and material incidents affecting a person within both mandates, and may issue joint circulars, conduct joint examinations and maintain a joint register of persons authorised by either authority.

4.7 **Disclosure of Scope in Approvals:** Every licence, authorisation or approval granted under these Regulations shall state the activities and Regulated Tokens it covers and that it does not authorise activities regulated by another authority.

4.8 **Delineation Matrix:** The allocation of activities between the Bank and the SEC is illustrated in the matrix in Schedule 8, which shall be read subject to this Section and to any Harmonised Implementation Framework adopted under the Presidential Executive Order on Virtual Assets Coordination, 2026.

4.9 **Custody and Wallet Services for Trading Purposes:** The holding, safeguarding, administration or Control of virtual assets, private keys, seed phrases, signing infrastructure or other access credentials solely for trading, brokerage, dealing, exchange, investment, capital market settlement or safekeeping purposes shall not, without more, constitute a Non-Security Virtual Asset Payment Activity and shall remain subject to the requirements of the SEC. Such an arrangement shall constitute a Non-Security Virtual Asset Payment Activity, requiring a licence or authorisation under Section 9, where it also:

a) receives or holds an Approved Virtual Asset Payment Instrument for payment purposes;

b) transfers or transmits an Approved Virtual Asset Payment Instrument on behalf of a customer[, other than a transfer to or from the customer's own wallet that is incidental to a trading or investment activity];

c) facilitates merchant acceptance or payment processing;

d) facilitates remittance, or the clearing or settlement of payment obligations;

e) provides stored-value functionality; or

f) otherwise performs a function within the mandate of the Bank.

4.10 Listing does not authorise payment use. The listing, admission to trading, brokerage, dealing, exchange or custody of a stablecoin or other virtual asset by a person regulated by the SEC shall not, by itself, authorise the use of that asset for payment, transfer, settlement, remittance, merchant-acceptance or stored-value purposes. Such use shall be subject to Section 9.13.

Section 5 Exemptions

5.1 The exclusions set out in Part 1 apply according to their terms. The Bank may specify an exemption by notice identifying its scope and conditions. An exemption shall not authorise securities business, remove obligations imposed by law or create an alternative to the Issuer Licence and Nigerian incorporation requirements for a stablecoin issuer.

5.2 A person relying on an exemption shall keep evidence supporting its application and provide that evidence to the Bank upon request. Where the relevant facts, functionality or conditions change, the person shall notify the Bank and obtain any licence, authorisation or Token Approval required before undertaking the changed activity.

5.3 The Bank may review an exemption and require an application for the appropriate licence, authorisation or Token Approval where the activity no longer satisfies its terms. Bank-issued digital currency, including the Central Bank Digital Currency, remains excluded. Deposit Money Tokens are subject to Part 10, and an Issuing Bank does not require an Issuer Licence merely because a deposit is tokenised.

Part 4
Licensing and Authorisation

Section 6 Licence Categories

6.1 No person shall carry on a Regulated Activity in or from Nigeria, or direct a Regulated Activity at persons in Nigeria, unless the Bank has granted that person the licence or authorisation required for that activity under this Section.

6.2 The licence and authorisation categories shall be:

a) Naira-referenced Issuer Licence (Class 1), authorising the issuance of Class 1 Stablecoins that have received Token Approval;

b) Foreign Currency Issuer Licence (Class 2), authorising the issuance of Class 2 Stablecoins that have received Token Approval;

c) Other Services Licence, permitting a person that does not hold a SEC licence to provide one or more non-issuance services specified by the Bank under Section 9;

d) Other Services Authorisation, permitting a person that holds a SEC licence for securities-related virtual asset services to provide one or more non-issuance services specified by the Bank under Section 9; and

e) Approval to Extend Permitted Activities, permitting a financial institution licensed by the Bank to undertake one or more Non-Security Virtual Asset Payment Activities as an extension of its Principal Licence under Section 9.6.

6.3 The Naira-referenced Issuer Licence (Class 1) and the Foreign Currency Issuer Licence (Class 2) are issuer categories. The classification of a token as a Class 1 Stablecoin or a Class 2 Stablecoin shall be determined by the Bank under Section 3.3. A token shall not be placed in either category merely because it is a Non-Security Virtual Asset. An Other Designated Token shall be subject to the activities and conditions specified by the Bank in its designation notice under Section 3.11.

6.4 A person holding a valid SEC licence for securities-related virtual asset services shall obtain an Other Services Authorisation before providing non-issuance services in relation to Non-Security Virtual Assets. A person without such a SEC licence that proposes to provide only such services shall obtain an Other Services Licence. A financial institution licensed by the Bank whose Principal Licence is relevant to the proposed activity may instead apply for an Approval to Extend Permitted Activities under Section 9.6 in respect of Non-Security Virtual Asset Payment Activities. An Other Services Licence, an Other Services Authorisation and an Approval to Extend Permitted Activities do not authorise issuance, for which a Naira-referenced Issuer Licence (Class 1) or a Foreign Currency Issuer Licence (Class 2) is required.

6.5 Every Class 1 Licensed Issuer shall be incorporated in Nigeria and hold a Naira-referenced Issuer Licence (Class 1). A foreign-currency-referenced stablecoin may be offered, marketed, distributed, exchanged, held in custody, redeemed or otherwise made available to persons in Nigeria only as a Class 2 Stablecoin issued through a Nigerian-incorporated entity holding a Foreign Currency Issuer Licence (Class 2). A foreign licence, registration, approval, regulatory status or arrangement with a Nigerian intermediary shall not substitute for that licence or for Token Approval. A Licensee shall not make available a stablecoin that has not received Token Approval.

6.6 A licence or authorisation is exclusive to its holder and non-transferable. Its scope shall be limited to the approved activities, Regulated Tokens, arrangements and conditions stated in it. No person shall hold both a Naira-referenced Issuer Licence (Class 1) and a Foreign Currency Issuer Licence (Class 2) without the Bank's express prior written approval.

6.7 A licence or authorisation granted under this Section authorises only activities within the Bank's mandate. A Licensee shall obtain and maintain every other licence required under applicable laws for its business. A licence or authorisation granted under these Regulations does not confer authority to conduct securities or other capital market business assigned by law to SEC.

6.8 Deposit Money Tokens issued by an Issuing Bank shall remain subject to Part 10. The Naira-referenced Issuer Licence (Class 1) and the Foreign Currency Issuer Licence (Class 2) shall not, merely by reason of tokenisation, convert a bank deposit liability into a stablecoin or replace the approvals required for Deposit Money Token activities under Part 10.

6.9 Form of licence or authorisation. The Bank may grant a licence or authorisation under this Section in the form of a licence, approval, authorisation, no-objection or endorsement of an existing licence, having regard to the applicant's existing regulatory status, the nature and scale of the proposed activity, the risks associated with it and whether the activity is ancillary to an existing business regulated by the Bank. Whatever its form, a licence or authorisation shall be limited to the activities expressly approved by the Bank and shall comply with Section 4.7.

Section 7 Issuer Licence Conditions and Application Requirements

Legal Form, Capital Documentation and Nigerian Incorporation

7.1 Promoters of a proposed issuer, or an incorporated applicant, may apply for an Approval-in-Principle for a Naira-referenced Issuer Licence (Class 1) or a Foreign Currency Issuer Licence (Class 2). At the application stage, the applicant or promoters shall:

a) be, or propose to be, a body corporate to be incorporated under the Companies and Allied Matters Act, 2020;

b) maintain, or submit arrangements to establish before final licensing, its principal place of business and a staffed physical office in Nigeria from which its key management functions will be exercised;

c) demonstrate how it will meet Sections 15 to 17, disclose the source of funds and provide evidence of capital deposited and the corresponding RTGS transfer where already made; the full applicable capital requirement and deposit shall be satisfied and evidenced before final licensing;

d) submit the prescribed application letter, documents and information, and evidence of payment of the non-refundable application fee prescribed in Schedule 3;

e) disclose actual or proposed legal and beneficial ownership, group structure, persons of significant control, directors and senior management and satisfy the assessment requirements in Section 18; and

f) identify every token for which Token Approval is sought, its class, reference currency, name, ticker symbol and blockchain networks, and each proposed distribution partner, which shall be a Licensee.

7.1.1 Promoters may apply for AIP before incorporation, identifying the proposed entity and the promoters responsible for the application. No final Issuer Licence shall be granted until the applicant has been incorporated in Nigeria under the Companies and Allied Matters Act, 2020 and has submitted the certified corporate documents required under Section 7.6(a).

7.2 The applicant shall demonstrate that it meets, or will meet before the Issuer Licence is granted under Section 8.6, all ongoing requirements of these Regulations applicable to a Licensed Issuer, including governance, capital, operational liquidity, reserve management, redemption, technology, payment security, operational resilience, business conduct, customer protection and AML/CFT/CPF controls.

7.3 The applicant shall demonstrate arrangements that will ensure, before final licensing and throughout operations, effective Nigerian management and supervisory access, including a resident Chief Compliance Officer, finance and reserve reporting, customer and redemption operations, access to records in Nigeria and authority to comply with lawful directions without prior offshore-parent approval.

7.4 A Class 1 Stablecoin shall reference the Naira on a one-to-one basis and be fully backed by Naira-denominated Eligible Reserve Assets. A Class 2 Stablecoin shall reference a foreign currency and comply with the applicable foreign-exchange, reserve, liquidity and redemption requirements. Issuance of a token shall not commence until the Bank has granted Token Approval, including approval of its reference currency and reserve arrangements.

7.5 Token Approval of a Class 2 Stablecoin shall not permit its use to settle, price or discharge a domestic obligation denominated in Naira, except where expressly permitted under applicable foreign-exchange or other law.

Legal Form, Capital Documentation and Nigerian Incorporation

7.6 The applicant shall submit:

a) where the applicant has been incorporated, certified true copies of its certificate of incorporation, memorandum and articles of association and relevant corporate filings; or, where the applicant has not yet been incorporated, draft constitutional documents, including the proposed memorandum and articles of association, together with such incorporation documentation and information as the Bank may require;

b) its proposed ownership and group structure, particulars of its proposed ultimate beneficial owners, persons of significant control, directors and significant shareholders, together with completed fit and proper questionnaires for such persons;

c) a three-year business plan covering token design, target markets, projected circulation, distribution channels, revenue model, financial projections, capital, liquidity, reserve management and redemption arrangements;

d) a Whitepaper for each token for which Token Approval is sought, complying with the requirements of Schedule 5, together with proposed customer terms, risk disclosures, fee schedules and complaints arrangements;

e) audited financial statements for the preceding two financial years, or management accounts where incorporated for less than two years; promoters of an unincorporated applicant shall submit opening financial projections and evidence of proposed funding and source of funds, with evidence of paid-up capital and the required deposit before final licensing;

f) a governance and risk management framework covering internal controls, accounting, compliance, internal audit, operational risk, technology, cybersecurity, liquidity, the Reserve Pool and concentration risk, approved by the board where constituted or submitted in draft by the promoters for adoption by the board before final licensing;

g) an AML/CFT/CPF programme covering customer and business due diligence, beneficial ownership, sanctions screening, transaction monitoring, suspicious transaction reporting, record retention and Travel Rule compliance;

h) a description of the issuance platform, smart contracts, minting and burning controls, private-key management, access controls, transaction monitoring and settlement arrangements;

i) the scope and provider of the independent smart contract security audit required under paragraph 10B of the Annex, together with any audit report already completed and the applicant's response to identified deficiencies;

j) executed agreements or term sheets with reserve banks, custodians, distribution partners and material service providers, identifying responsibilities, access rights and arrangements for termination and continuity;

k) policies governing the management, valuation, reconciliation, segregation, liquidity and redemption of the Reserve Pool, together with an independent Nigerian legal opinion confirming the enforceability of the Reserve Pool segregation arrangements and the priority rights of holders in relation to the Reserve Pool;

l) evidence of appointment, or proposed engagement, of an Approved Independent Auditor for reserve attestations, with appointment confirmed before final licensing;

m) business continuity, disaster recovery, incident response, recovery and orderly wind-down plans, including arrangements to protect assets and meet outstanding redemption obligations;

n) the independent assessments required by Section 7.7; and

o) any further information, legal opinion, assurance or evidence required by the Bank to determine the application.

Independent Assessments

7.7 The applicant shall submit with its application for Approval-in-Principle the independent assessments listed in paragraph 10A of the Annex. The assessments listed in paragraph 10B of the Annex shall be submitted and found satisfactory before the Bank grants the Issuer Licence under Section 8.6. Each assessment report shall not be more than six months old at submission.

7.8 Assessors shall be competent, suitably qualified and independent of the business units and operations reviewed. They shall not have selected or implemented the controls they assess, shall have relevant knowledge and experience, and shall confirm to the Bank their independence and absence of conflicts of interest. Reports shall identify their scope, methods, evidence, findings, deficiencies and conclusions. The applicant shall submit a remediation plan and evidence of closure of deficiencies required by the Bank before the Issuer Licence is granted.

7.9 The Bank may require updated assessments where the application remains pending, arrangements change materially or the reports no longer provide adequate assurance. Pre-licensing assessments shall not replace the ongoing reserve attestations, annual financial audits, technology reviews or other assurance required of a Licensed Issuer by these Regulations.

7.10 An applicant forming part of a foreign group shall provide details of relevant foreign regulators, existing regulatory approvals, restrictions, enforcement actions and arrangements for existing regulatory and supervisory cooperation.

7.11 Foreign regulatory oversight shall supplement, and shall not displace, the Nigerian incorporation, capital, licensing and ongoing requirements applicable to a Licensed Issuer.

Section 8 Issuer Licensing Procedure and Approval-in-Principle

8.1 **Preliminary meeting:** The Bank may avail prospective applicants the opportunity to have preliminary meetings and discussions as regards the proposed business, token classification, ownership, reserve structure, redemption arrangements and application requirements before formal submission. The Bank may meet separately with directors, persons of significant control and senior management as it deems fit. A preliminary meeting shall not constitute an approval to operate.

8.2 **Submission:** The applicant or promoters shall submit the prescribed application for AIP, documents, application-stage assessments, certifications and application fee. The submission shall distinguish existing arrangements from proposed arrangements and identify matters to be completed after AIP. Material changes shall be disclosed immediately to the Bank.

8.3 **Regulatory Consultation:** Where the applicant or the parent company is regulated by another authority, the Bank may consult that authority, including SEC or a relevant foreign regulator, regarding regulatory standing, fitness and propriety, group risks and supervisory cooperation. The applicant shall provide the information and consents necessary for such consultation.

8.4 **Processing:** The Bank shall assess the application against these Regulations and may require additional documents, explanations, interviews, independent reviews, demonstrations or inspections. An incomplete application shall be identified in writing and the applicant required to remedy deficiencies within a period specified by the Bank. Processing may be suspended by written notice until outstanding information is supplied. An application suspended for six months or more shall require a fresh application if the applicant wishes to proceed.

8.4.1 The Bank shall communicate its decision on a complete application in writing. Where additional information, documents, clarifications, interviews, demonstrations or remediation are required, assessment shall remain pending until the Bank is satisfied with the response.

8.5 **Approval-in-Principle:** Following assessment, the Bank may grant AIP, subject to specified conditions, where satisfied that the applicant or promoters are suitable and that the proposed business can meet the applicable licensing requirements. An AIP may be granted before incorporation.

8.5.1 An Approval-in-Principle shall not constitute a licence and shall not authorise the holder to commence operations or undertake any regulated activity requiring authorisation under these Regulations.

8.5.2 The applicant or promoters shall fulfil the conditions of AIP, including incorporation where outstanding and completion of applicable legal, governance, capital, liquidity, reserve, custody, technology, cybersecurity, reporting, consumer-protection and operational requirements.

8.5.3 Before granting the final licence, the Bank shall verify operational readiness and compliance with the applicable conditions. It may conduct inspections, system reviews, testing, demonstrations and validation exercises and require the independent assessments and remediation evidence prescribed by Sections 7.7 to 7.9.

8.5.4 Where an Approval-in-Principle is granted to an applicant that has not yet been incorporated, the applicant shall, prior to the grant of a licence, provide evidence of incorporation, constitutional documents and any other corporate filings required by the Bank.

8.5.5 An Approval-in-Principle shall remain valid for such period as may be specified by the Bank and may be extended, varied, suspended or withdrawn by the Bank where the applicant fails to satisfy applicable conditions or where circumstances warrant such action.

8.6 Final licence and commencement: The Bank may grant the Issuer Licence only after the applicant has obtained an AIP, fulfilled its conditions, been incorporated in Nigeria and satisfactorily completed operational-readiness verification and all applicable pre-licensing requirements. Operations shall commence only after the final licence and relevant Token Approval have been granted and all applicable pre-commencement conditions have been met.

8.6.1 Subject to the applicant's assessed risk profile, the Bank may adjust capital or liquidity requirements or reserve safeguards, impose activity restrictions, limits on circulation or customers, or other appropriate conditions.

8.7 **Licence Particulars:** The licence shall identify the Licensee, licence class, the Regulated Token or Tokens covered by Token Approval, authorised activities, unique reference number, effective date, validity period and applicable conditions.

8.7.1 The Bank shall maintain and publish a register of every licence, authorisation and approval granted under these Regulations, specifying for each the holder, the activities and Regulated Tokens covered, any material conditions, and the date and status, including suspension or revocation. The register shall be accessible to the public and to foreign competent authorities. The list of unauthorised persons under Section 52.6 shall be published with it.

8.7.2 The Licensee shall display its regulatory status and reference number on its website and relevant documents.

8.7.3 The displayed notice specified in 8.7.2 shall clearly indicate that the Bank does not guarantee the token or its obligations.

8.8 **Changes:** A Licensee shall obtain the Bank's prior written approval before any change of ownership, control or fundamental business model, or any expansion beyond its approved licence scope. Proposed new tokens and material changes to approved issuance or reserve arrangements shall be submitted to the Bank before implementation.

Section 9 Licensing and Authorisation for Other Non-Security Virtual Asset Services

9.1 **Covered Services:** A licence or authorisation under this Section may cover one or more of the following activities, to the extent of the Bank's mandate:

a) **Custody and Custodial Wallet Services:** Holding, safeguarding or administering, for or on behalf of a customer, Non-Security Virtual Assets, private keys or other instruments that enable the provider to access or exercise control over such assets, including through a custodial or hosted wallet;

b) **Non-Custodial Wallet Services:** Providing or operating a wallet service that enables a customer to hold, store, access, receive, transfer, redeem or otherwise manage Non-Security Virtual Assets, where the customer retains sole control of the private keys or other means of controlling those assets;

c) **Exchange, Conversion, Transfer and Remittance Services:**

i) buying, selling, exchanging or converting, for or on behalf of a customer, Non-Security Virtual Assets for Naira or other fiat currency, or for other virtual assets; and

ii) facilitating, processing, routing, clearing or settling domestic or cross-border transfers, remittances or payments involving Non-Security Virtual Assets;

d) **Token Distribution:** Distributing or facilitating access to Regulated Tokens issued by a Licensed Issuer, without assuming the role of issuer;

e) **Virtual Asset Payment Gateway Services:** Providing payment gateway, merchant-acquiring or payment-acceptance services involving Approved Virtual Asset Payment Instruments;

f) **Virtual Asset Stored-Value Facilities:** Operating facilities that hold Approved Virtual Asset Payment Instruments for customers to make future payments or transfers;

g) **Platform-Facilitated Peer-to-Peer Services:** Operating or facilitating a P2P Service, subject to the approval and requirements of Section 10; and any further activity designated by the Bank.

9.2 **Licensing and Authorisation Routes:** A person proposing to provide a service in Section 9.1 shall, before commencing the service, obtain:

a) where it is licensed, registered, approved or otherwise regulated by the SEC, an Other Services Authorisation under Section 9.4;

b) where it is a financial institution licensed by the Bank and the service is a Non-Security Virtual Asset Payment Activity within the scope of its Principal Licence, an Approval to Extend Permitted Activities under Section 9.6; or

c) in any other case, an Other Services Licence under Section 9.5.

A person regulated by both the Bank and the SEC shall apply under paragraph (b) for Non-Security Virtual Asset Payment Activities and under paragraph (a) for any other service in Section 9.1, unless the Bank directs otherwise. The routes are summarised in Part C of Schedule 8.

9.3 **Conditions:** An applicant shall be incorporated in Nigeria before final licensing or authorisation, maintain effective physical and management presence in Nigeria, meet Sections 16 and 17, satisfy Section 18 and demonstrate resources, controls and resilience appropriate to its services. Promoters of a proposed standalone Other Services Licence applicant may apply for AIP before incorporation; the staged documentary requirements in Section 7 and procedure in Section 8 apply with necessary modifications. An Other Services Authorisation applicant shall hold the SEC licence required by Section 9.4. An applicant for an Approval to Extend Permitted Activities is subject to Section 9.6.4 instead of the incorporation, AIP and capital requirements of this Section. Section 7.3 applies to an applicant for an Other Services Licence, with necessary modifications, and the applicant shall in particular maintain a Chief Compliance Officer and a Money Laundering Reporting Officer resident in Nigeria with unrestricted access to customer, wallet and transaction data, including data held by any group entity outside Nigeria.

9.4 **SEC Licensees:** An applicant holding a valid SEC licence for securities-related virtual asset services intending to apply for an Other Services Authorisation shall submit

a) a copy of the SEC licence,

b) approved service scope

c) regulatory conditions; and

d) relevant supervisory history.

9.4.1 The Bank shall coordinate with SEC in assessing overlapping activities and supervisory responsibilities.

9.4.2 The Other Services Authorisation shall be documented as a specific approval or endorsement of the applicant's existing regulatory status but shall expressly identify the non-security services approved by the Bank.

9.4.3 **Reliance on SEC Assessments:** In assessing an application from a SEC licensee, the Bank may rely on the SEC's fit and proper, governance and AML/CFT/CPF assessments, subject to any update the Bank considers necessary, and shall confine its review to matters within its mandate, including payment, settlement, custody of value used for payment, foreign-exchange and reserve arrangements. The Bank and SEC shall exchange information on the application under Section 4.6.

9.4.4 An applicant for an Other Services Authorisation shall demonstrate that it has

a) a valid SEC licence, registration or approval for its underlying virtual asset activity;

b) adequate governance and risk-management arrangements;

c) systems for safeguarding and segregating customer funds and assets;

d) appropriate technology, cybersecurity and operational-resilience controls;

e) effective AML/CFT/CPF and sanctions-screening controls;

f) transaction-monitoring and reporting systems;

h) adequate arrangements for customer complaints and redress; and

9.4.5 A licence, registration or approval granted by the SEC shall not, by itself, authorise the holder to provide a service in Section 9.1.

9.5 **Exclusive Non-security Providers:** An applicant without a relevant SEC licence that desires to provide exclusively Non-Security Virtual Asset services shall apply for an Other Services Licence. If it subsequently proposes securities-related services, it shall first obtain the approvals required from SEC and the Bank's approval for the change in its business scope.

9.6 **Existing CBN-regulated Institutions:** A financial institution licensed and regulated by the Bank may apply for an Approval to Extend Permitted Activities to undertake one or more Non-Security Virtual Asset Payment Activities where it holds a valid Principal Licence relevant to the proposed activity, including a licence for deposit-taking, electronic-money issuance, mobile money or wallet services, payment services, transfer services, international money transfer or remittance services, switching, clearing or settlement.

9.6.1 An institution granted an Approval to Extend Permitted Activities shall not require a separate Other Services Licence or Other Services Authorisation for the activities covered by the approval. The approval shall be limited to the specific activities, Approved Virtual Asset Payment Instruments, channels and conditions expressly approved by the Bank and shall be read with the limitations of the Principal Licence.

9.6.2 An Approval to Extend Permitted Activities shall not authorise the issuance of stablecoins, for which an Issuer Licence is required, the issuance of Deposit Money Tokens, which is governed by Part 10, or virtual asset exchange, brokerage, dealing, trading, investment, custody (other than custody through a Custodial Virtual Asset Payment Wallet), listing or offering, or any other activity within the statutory mandate of the SEC, except that custody, and exchange or conversion, of an Approved Virtual Asset Payment Instrument undertaken as part of an approved Non-Security Virtual Asset Payment Activity are not excluded by this paragraph.

9.6.3 The applicant shall submit, through the department of the Bank responsible for supervising its Principal Licence,

a) a board-approved application identifying each proposed activity, Approved Virtual Asset Payment Instrument, customer segment, channel and settlement route;

b) a gap assessment against Sections 9.8, 25 and 26 and Parts 8 and 9;

c) an AML/TF/PF risk assessment of the proposed activity;

d) the technology, key-management, safeguarding and reconciliation arrangements for any Custodial Virtual Asset Payment Wallet;

e) any outsourcing arrangements; and

f) the independent assessments under Section 9.9 applicable to the proposed activity.

The Bank may rely on information it already holds in respect of the Principal Licence.

9.6.4 The incorporation and Approval-in-Principle requirements of Section 9.3 shall not apply to an application under this Section. The applicant shall continue to meet all capital and other prudential requirements applicable under its Principal Licence and shall, in addition, meet the capital requirements for Other Non-Security Virtual Asset Services under Sections 16 and 17. The Bank may impose additional requirements relating to:

a) the safeguarding and segregation of customer funds and assets;

b) capital and liquidity;

c) reserves or collateral;

d) operational and technology risk;

e) cybersecurity;

f) consumer protection;

g) transaction monitoring;

h) business continuity;

i) reporting and record keeping; and

j) audit and supervisory access.

9.6.5 Section 8 shall apply to the processing of an application under this Section with the necessary modifications, save that an Approval-in-Principle shall not be required unless the Bank so directs.

9.7 Application requirements:

a) application letter;

b) incorporation documents, or draft memorandum and articles of association and proposed incorporation particulars for a promoter AIP application, followed by certified incorporation documents before final licensing;

c) actual or proposed ownership and management particulars;

d) fit and proper questionnaires;

e) a three-year business plan;

f) financial statements or management accounts where available, or opening financial projections and proposed funding information for an unincorporated applicant;

g) source-of-funds information and evidence of the required capital deposit and RTGS transfer, where already made, with full compliance before final licensing;

h) the AML/CFT/CPF programme;

i) the risk and governance framework;

j) technology and security documentation;

k) customer terms and conditions of service;

l) asset-protection arrangements;

m) material outsourcing agreements;

n) business continuity plans;

o) wind-down plans; and

p) the prescribed fees.

The application shall identify each proposed token, service, issuer, distribution, arrangements and settlement route.

9.8 Activity-specific requirements:

9.8.1 A custodian or wallet provider controlling customer assets shall demonstrate segregation, reconciliation, secure key management, recovery arrangements and a prohibition on use of client assets for its own purposes.

9.8.2 Exchange and on-ramp or off-ramp providers shall demonstrate pricing and execution controls, transaction monitoring and compliance with approved foreign-exchange channels.

9.8.3 Transfer, payment and settlement providers shall demonstrate operational resilience, reconciliation and legally effective settlement arrangements.

9.8.4 A provider of Virtual Asset Payment Gateway Services or merchant-acceptance services shall demonstrate merchant due diligence and monitoring, settlement to merchants within the timeframe approved by the Bank, refund and chargeback arrangements, and the conversion and settlement routes used.

9.8.5 A provider of a Virtual Asset Stored-Value Facility shall safeguard customer balances in accordance with Section 25, shall not pay interest or yield on those balances and shall enable customers to redeem or transfer their balances without undue delay.

9.8.6 A provider of cross-border transfer or remittance services shall demonstrate compliance with Section 9.14.

The application shall identify each proposed token, service, issuer, distribution, arrangements and settlement route.

9.9 **Independent Assessments:** The applicant shall provide independent assessments not more than six months old covering the areas in paragraphs 10A and 10B of the Annex at the corresponding application and pre-licensing stages to the extent applicable to its services. Any area considered inapplicable shall be expressly identified and justified for the Bank's determination. A provider that does not manage issuer reserves shall nevertheless demonstrate the adequacy of safeguards for any customer assets or funds it controls. The independence and remediation requirements in Section 7.8 and Section 7.9 shall apply.

9.10 **Procedure:** The preliminary meeting, submission, regulatory consultation, processing, Approval-in-Principle, final approval, register and change-approval procedures in Section 8 shall apply with the necessary modifications. An existing CBN licence, a SEC or other regulator licence, or Submission of a notification shall not, by itself, authorise a new non-security virtual asset service; provided that a financial institution licensed by the Bank may obtain approval to extend its permitted activities under Section 9.6. The Bank's express written licence or authorisation shall be required before commencement of such activities.

9.11 **Scope Limitations:** The approval shall specify the services, tokens, customers, channels and conditions covered. Distribution of a Class 2 Stablecoin shall be approved within the provider's non-issuance licence or authorisation and shall not confer issuer status. A service provider shall not mint tokens on its own account or assume the role of issuer without the appropriate Issuer Licence. Outsourcing shall not transfer regulatory responsibility from the approved entity.

9.12 **Lending and Borrowing:** A licence or authorisation under this section shall not of itself authorise lending or borrowing of Non-Security Virtual Assets. Such activity may be undertaken only under a separate approval required by applicable law from the Bank or other competent authority. No such approval shall permit the use of issuer reserves or customer assets contrary to these Regulations.

9.13 **Payment Use of Regulated Tokens:** No person shall facilitate the use of a stablecoin or other virtual asset for payment, transfer, settlement, remittance, merchant-acceptance or stored-value purposes unless (a) it is an Approved Virtual Asset Payment Instrument; and (b) the person holds the licence or authorisation required under this Section for the relevant activity. The Bank may approve, restrict, suspend or prohibit the payment-related use of a Regulated Token where it considers this necessary in the interest of monetary stability, financial stability, payment-system integrity, foreign-exchange integrity, consumer protection, financial integrity or the safety and soundness of the financial system. Approval of a token for payment-related use shall not constitute an endorsement or guarantee by the Bank of the token, its issuer, its value, its reserves or its convertibility.

9.14 **Cross-border Transfers and Remittances:** No person shall provide cross-border transfer or remittance services involving an Approved Virtual Asset Payment Instrument without the express approval of the Bank for that activity. An approved person shall comply with all applicable requirements relating to foreign-exchange administration in Nigeria, AML/CFT/CPF obligations, customer due diligence and enhanced due diligence,

sanctions screening, originator and beneficiary information under the Travel Rule, transaction monitoring, suspicious transaction and other regulatory reporting, record keeping, consumer disclosures, and complaints handling and redress, including Sections 11.7 and 26.

9.15 **Conditions:** The Bank may grant a licence or authorisation under this Section subject to conditions, including restrictions on the Approved Virtual Asset Payment Instruments that may be used, the class of customers that may be served, transaction value and frequency, geographic coverage, settlement arrangements, customer-fund or asset exposure, cross-border activity and the duration or pilot nature of the approval, where necessary to protect financial or monetary stability, payment-system integrity, consumer interests, the safety and soundness of regulated institutions or the integrity of the financial system.

Section 10 Platform-Facilitated Peer-to-Peer Services

10.1 Purpose and Scope

10.1.1 This Section establishes the requirements applicable to the operation or facilitation of Platform-Facilitated Peer-to-Peer Services involving Regulated Tokens.

10.1.2 A Platform-Facilitated Peer-to-Peer Service may include matching counterparties, displaying orders, facilitating the purchase, sale or exchange of a Regulated Token, providing escrow or transaction safeguards, facilitating payment, transfer, clearing, reconciliation or settlement, verifying transactions, or providing dispute-resolution services.

10.1.3 This Section applies to the virtual-asset leg and, where applicable, the Naira, payment, settlement or other fiat leg of a P2P transaction, whether the relevant virtual-asset transaction is recorded on-chain, off-chain or through an internal ledger or other system operated by or on behalf of the provider.

10.1.4 This Section does not apply to a purely private bilateral transfer between persons where no person other than the transacting parties operates, facilitates, intermediates, matches, safeguards, settles or otherwise supports the transaction.

10.2 Authorisation

10.2.1 The Bank shall not grant a separate licence category solely for the provision of Platform-Facilitated Peer-to-Peer Services.

10.2.2 A person shall not operate, facilitate or hold itself out as providing a P2P Service unless:

a) it holds the applicable Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities under Section 9; and

b) the Bank has expressly approved Platform-Facilitated Peer-to-Peer Services within the scope of that licence, authorisation or approval.

10.2.3 An approval under this Section shall identify, or permit the Bank to prescribe, the Regulated Tokens (which may include Class 1 Stablecoins and Class 2 Stablecoins), customer categories, transaction types, payment or settlement arrangements, geographic scope and other conditions applicable to the P2P Service.

10.2.4 A licence, authorisation or approval permitting another Other Non-Security Virtual Asset Service shall not, by itself, authorise the provision of a P2P Service.

10.2.5 A P2P Service provided under an Approval to Extend Permitted Activities is limited to Approved Virtual Asset Payment Instruments.

10.2.6 A person that does not itself hold the approval required under this Section shall not independently operate or hold itself out as the provider of a P2P Service.

10.2.7 A licensed or authorised provider may use an agent, distributor, technology provider or outsourced service provider in connection with an approved P2P Service only in accordance with Sections 21 and 22 and any prior approval required by the Bank. The licensed or authorised provider shall remain fully responsible for the P2P Service and for compliance with these Regulations.

10.3 Customer Identification and Access Controls

10.3.1 A provider of a P2P Service shall ensure that every customer using the service is subject to applicable customer identification, verification, customer due diligence and ongoing monitoring requirements before being permitted to transact.

10.3.2 The provider shall maintain sufficient information to identify each customer and counterparty participating in a P2P transaction and to attribute each transaction to the relevant customer accounts, wallets, payment accounts and settlement arrangements.

10.3.3 A provider shall not release or credit a Regulated Token in a P2P transaction unless it has verified that the name and the Bank Verification Number of the account from which the Naira payment was made, or to which it was made, match the verified customer on whose behalf the provider acts. The Bank may prescribe further requirements relating to payment-account verification, permitted customer categories, transaction and customer limits, and other controls.

10.3.4 A provider shall not knowingly permit the use of third-party, nominee, mule, fictitious or otherwise improperly attributed accounts or wallets for the purpose of concealing the identity of a customer, counterparty, beneficiary or source or destination of funds or value.

10.3.5 **Business users:** A provider shall maintain criteria, approved by its board and notified to the Bank, for identifying a customer that buys, sells or exchanges Regulated Tokens on the P2P Service as a business, having regard to transaction volume, frequency, number of counterparties and advertising of rates. The provider shall apply enhanced due diligence and transaction limits to such customer and report the customer to the Bank under Section 10.8. Such identification shall not constitute authorisation to conduct a regulated activity. A customer conducting an activity requiring authorisation shall obtain the applicable licence or authorisation, cease the activity, or operate as an agent of the provider under Section 21, as the Bank may direct.

10.4 Operating Requirements

10.4.1 A provider of a P2P Service shall:

a) maintain systems and controls appropriate to the nature, scale and complexity of the service;

b) maintain systems and records sufficient to link and reconcile the virtual-asset leg of each transaction with the corresponding Naira, payment or settlement leg;

c) record the relevant customers and counterparties, transaction value, exchange or conversion rate, payment or settlement reference, wallet addresses or account identifiers and such other information as the Bank may prescribe;

d) maintain transaction-monitoring, fraud-prevention, sanctions-screening and AML/CFT/CPF controls appropriate to the P2P Service;

e) maintain procedures for identifying failed, incomplete, disputed, fraudulent or anomalous transactions;

f) maintain appropriate controls governing order matching, escrow, transaction verification, release of virtual assets and dispute resolution; and

g) comply with any transaction, customer, volume, concentration, geographic, token-specific or other limits prescribed by the Bank.

10.5 Naira Payment and Settlement

10.5.1 Where a P2P transaction includes a Naira payment or settlement leg, that leg shall be effected through a Nigerian banking, payment or other settlement channel permitted by the Bank, unless the Bank has expressly approved another arrangement.

10.5.2 Paragraph 10.5.1 does not require the P2P provider itself to receive, hold or transmit the Naira consideration where payment is made directly between verified customers through permitted Nigerian banking or payment channels, provided that:

a) the transaction remains subject to the provider's systems, controls and monitoring;

b) the provider can identify the originator and beneficiary;

c) the provider can link and reconcile the Naira payment or settlement leg with the corresponding virtual-asset leg; and

d) the provider maintains the records and information required under this Section.

10.5.3 A provider that supports settlement of a P2P transaction, including by controlling a virtual asset in escrow pending completion of the corresponding payment leg, shall maintain clear rules governing when each leg is treated as initiated, completed, failed, cancelled or final and shall comply with the applicable requirements of Section 34.

10.5.4 Where the provider controls virtual assets in escrow or otherwise has Control of customer assets during a P2P transaction, it shall comply with the applicable safeguarding, segregation and reconciliation requirements under Section 25.

10.6 Foreign-Exchange Requirements and Anti-Circumvention

10.6.1 Approval to provide a P2P Service shall not, of itself:

a) constitute authority to conduct foreign-exchange business;

b) create or authorise an alternative foreign-exchange market;

c) authorise the purchase, sale, conversion or transfer of foreign-currency value where that activity would otherwise require separate approval or would be restricted or prohibited under applicable law; or

d) disapply any foreign-exchange, capital-flow, payment, documentation, reporting or other requirement administered by the Bank.

10.6.2 A provider shall not facilitate a P2P transaction involving conversion between Naira and a Class 2 Stablecoin or other foreign-currency value unless the Bank has expressly approved that activity under Section 10.2.3. Any such approval shall require that:

a) the Naira leg is settled through, or reported to, an authorised dealer designated in the approval;

b) the transaction is reported for foreign-exchange monitoring in the form the Bank prescribes; and

c) such purposes, limits and documentation as the Bank prescribes are observed.

10.6.3 The use of a Regulated Token or P2P Service shall not alter the regulatory treatment of the underlying economic transaction or permit a person to undertake through a virtual asset a transaction that would not otherwise be permissible through conventional banking, payment or foreign-exchange channels.

10.6.4 No person shall structure, split, route, facilitate or use a P2P transaction or series of transactions for the purpose or effect of circumventing:

a) CBN oversight;

b) applicable foreign-exchange or capital-flow requirements;

c) transaction, customer, volume or other limits prescribed by the Bank;

d) documentation or permitted-purpose requirements;

e) AML/CFT/CPF or sanctions controls; or

f) regulatory reporting requirements.

10.6.5 The Bank may require a provider to obtain, verify and retain information relating to the purpose of a transaction, source and destination of funds or value, underlying commercial or personal transaction, originator and beneficiary, relevant jurisdictions and such supporting documentation as the Bank considers necessary for foreign-exchange, capital-flow, balance-of-payments or supervisory purposes.

10.7 AML/CFT/CPF, Sanctions and Travel Rule

10.7.1 A provider of a P2P Service shall comply with all applicable AML/CFT/CPF, targeted financial sanctions and financial-integrity requirements under Section 26 and applicable law.

10.7.2 Without limiting paragraph 10.7.1, the provider shall maintain controls covering:

a) Customer due diligence and ongoing monitoring;

b) beneficial-ownership identification where applicable;

c) sanctions and watchlist screening;

d) transaction and wallet monitoring;

e) suspicious transaction identification and reporting;

f) record keeping;

g) higher-risk customers, transactions, jurisdictions and counterparties; and

h) such other controls as may be prescribed by the Bank or the NFIU.

10.7.3 Where both parties to a P2P transaction are customers of the provider, the provider shall obtain, hold and retain the originator and beneficiary information required by Section 26.14.3 for the transfer, regardless of amount, and shall make it available to the Bank and the NFIU on request. Where a P2P transaction involves another VASP, Section 26.14 applies in full; where it involves an unhosted wallet, Section 26.15 applies.

10.7.4 Where the Travel Rule applies, the provider shall obtain, hold, verify where required, transmit and retain the prescribed originator and beneficiary information in accordance with applicable law and regulatory requirements.

10.7.5 A provider shall maintain appropriate controls to identify suspicious or anomalous P2P activity, including structuring, rapid movement of value, layering through multiple wallets or accounts, use of mule or third-party accounts, transaction splitting, unusual counterparty concentration, attempts to obscure the relationship between the fiat and virtual-asset legs, or activity structured to evade applicable requirements or reporting.

10.8 Reporting and Supervisory Visibility

10.8.1 A provider shall maintain complete and accurate transaction-level records sufficient to reconstruct and reconcile each P2P transaction, including its virtual-asset and fiat, payment or settlement legs.

10.8.2 The Bank may require periodic, event-driven, real-time or near-real-time reporting in respect of P2P Services.

10.8.3 Reporting prescribed by the Bank may include:

a) transaction volumes and values;

b) Naira inflows and outflows;

c) customer and counterparty categories;

d) exchange or conversion rates;

e) transaction purpose;

f) direction of flow;

g) payment and settlement references;

h) wallet addresses, transaction hashes and relevant account identifiers;

i) originator and beneficiary information;

j) domestic and cross-border flows;

k) failed, cancelled, disputed, fraudulent, suspicious or anomalous transactions;

l) concentration by customer, counterparty, token, financial institution, jurisdiction or settlement channel; and

m) any other information required for monetary policy, foreign-exchange administration, balance-of-payments monitoring, financial stability, payment-system supervision, AML/CFT/CPF, sanctions compliance, consumer protection or financial-integrity purposes.

10.8.4 The provider shall ensure that outsourcing, offshore processing, group arrangements, distributed-ledger architecture or direct customer-to-customer settlement does not prevent the Bank, the NFIU or another competent authority from obtaining information lawfully required for supervisory or enforcement purposes.

10.9 Cross-Border P2P Activity

10.9.1 An approval to provide a domestic P2P Service shall not constitute approval to provide a cross-border transfer or remittance service.

10.9.2 A provider that proposes to:

a) provide a P2P Service as a cross-border transfer or remittance service;

b) facilitate P2P transactions between a person in Nigeria and a counterparty outside Nigeria; or

c) otherwise facilitate the transfer or settlement of value across Nigeria's borders through a P2P arrangement,

shall obtain the Bank's approval for the relevant cross-border activity under Section 9.14.

10.9.3 Cross-border P2P activity shall comply with all applicable foreign-exchange, capital-flow, AML/CFT/CPF, sanctions, Travel Rule, reporting, record-keeping and consumer-protection requirements.

10.9.4 The Bank may impose additional conditions on cross-border P2P activity, including permitted corridors, jurisdictions, counterparties, tokens, transaction purposes, transaction and customer limits, settlement channels, documentary requirements and enhanced reporting.

10.10 Customer Protection, Escrow and Dispute Resolution

10.10.1 A provider shall disclose clearly to customers:

a) the nature of the P2P Service and the role of the provider;

b) whether and to what extent the provider controls, safeguards or escrows customer assets;

c) the mechanism for matching, payment, settlement and release of virtual assets;

d) applicable fees, spreads and exchange or conversion rates;

e) circumstances in which a transaction may be suspended, cancelled or reversed;

f) the procedures applicable to failed, disputed or fraudulent transactions; and

10.10.2 Where the provider operates an escrow arrangement, it shall maintain objective and transparent conditions governing the release, return or continued holding of the relevant virtual assets.

10.10.3 The provider shall maintain procedures for complaints, disputes, fraud claims, erroneous transactions and escalation to the Bank in accordance with the applicable customer-protection requirements under these Regulations.

10.11 Conditions, Restrictions and Supervisory Intervention

10.11.1 The Bank may attach conditions to an approval to provide a P2P Service, including conditions relating to:

a) permitted Regulated Tokens;

b) customer eligibility;

c) transaction value or frequency;

d) aggregate transaction or customer limits;

e) permitted banking, payment or settlement channels;

f) foreign-exchange treatment;

g) geographic scope and cross-border activity;

h) escrow or safeguarding;

i) reporting frequency and data access;

h) technology, operational or risk-management controls; and

i) pilot, testing or phased implementation requirements.

10.11.2 The Bank may impose additional requirements, vary existing conditions, restrict new transactions, restrict particular tokens, customers, counterparties, corridors or settlement channels, or suspend or withdraw approval for a P2P Service where the Bank considers this necessary for monetary stability, foreign-exchange integrity, financial stability, payment-system integrity, consumer protection, financial integrity, AML/CFT/CPF compliance or the safety and soundness of the financial system.

10.11.3 A provider shall comply promptly with any lawful direction issued by the Bank in respect of its P2P Service and shall maintain the operational and technical capability to implement restrictions, enhanced monitoring, reporting or other supervisory measures prescribed by the Bank.

Section 11 Additional Requirements for Class 2 Stablecoins

11.1 **Class 2 Eligibility and Market Access:** A Class 2 Stablecoin shall be issued only by a Nigerian-incorporated entity holding a valid Foreign Currency Issuer Licence (Class 2) granted by the Bank. No foreign-currency-referenced stablecoin shall be offered, distributed, marketed, exchanged, custody-held, redeemed or otherwise made available to persons in Nigeria unless it has been approved by the Bank as a Class 2 Stablecoin and is issued through a Class 2 Licensed Issuer.

11.2 **Foreign Sponsors and Affiliates:** A Class 2 Licensed Issuer may form part of, be controlled by, or act in association with a foreign issuer, foreign stablecoin arrangement or international group, provided that:

a) the Nigerian-incorporated Class 2 Licensed Issuer remains fully responsible for compliance with these Regulations;

b) the Bank has unrestricted supervisory access to the issuer, its books, records, systems, reserve arrangements and relevant group information;

c) the issuer demonstrates the existence of appropriate cooperation arrangements with relevant foreign regulators where required by the Bank; and

d) any foreign regulatory approvals, licences or supervision shall supplement and not replace compliance with these Regulations or any requirement imposed by the Bank.

11.3 **Operational Liquidity:** A Class 2 Licensed Issuer shall maintain Operational Liquidity that is legally and operationally accessible for the timely satisfaction of Nigerian redemption requests, payment obligations and other liabilities arising from its activities in Nigeria, including during a Stress Event.

11.3.1 A provider shall comply promptly with any lawful direction issued by the Bank in respect of its P2P Service and shall maintain the operational and technical capability to implement restrictions, enhanced monitoring, reporting or other supervisory measures prescribed by the Bank.

a) US$10,000,000 (ten million United States dollars), or its equivalent in the reference currency of the Class 2 Stablecoin;

b) fifteen per cent (15%) of the aggregate Nigeria-linked outstanding liabilities attributable to the Class 2 Stablecoin; and

c) the amount reasonably required to meet thirty (30) days of stressed Nigerian redemption requests, payment obligations and other expected liquidity outflows, calculated in accordance with a stress-testing methodology approved or prescribed by the Bank.

11.3.2 Nigeria-linked Outstanding Liabilities: For the purposes of this Section and Section 24.50, "Nigeria-linked outstanding liabilities" shall include Class 2 Stablecoins held, distributed, acquired, redeemed, transferred, used or otherwise attributable to persons in Nigeria, Nigerian customer accounts, Nigerian distribution channels or such other Nigerian activity as the Bank may prescribe. The Bank shall prescribe the methodology for attribution, valuation and calculation of such liabilities and may require an issuer to apply a conservative methodology where attribution cannot be determined with reasonable certainty.

11.3.3 Currency composition: Operational Liquidity shall be maintained predominantly in the reference currency of the relevant Class 2 Stablecoin.

Where necessary to support lawful Nigerian payment or settlement obligations, the Bank may permit a portion to be maintained in Naira or another approved currency, provided that such amount shall not impair the issuer's ability to meet redemption obligations in the reference currency.

11.3.4 Accessibility and protection: Operational Liquidity shall:

a) be unencumbered and free from any lien, charge, pledge, security interest or other restriction that could impair its availability;

b) be held through accounts, facilities or other arrangements approved by the Bank;

c) be legally and operationally available for Nigerian redemption and payment obligations without undue delay, including during a Stress Event;

d) be maintained separately from the issuer's required regulatory capital and separately from the Reserve Pool, and shall not be counted towards satisfaction of either requirement; and

e) be subject to the concentration, diversification, custody, replenishment and other prudential requirements prescribed by this Section or by the Bank.

11.3.5 Nigerian banking and custody arrangements: Unless otherwise approved by the Bank, Operational Liquidity shall be maintained through one or more designated accounts or liquidity arrangements with Deposit Money Banks licensed by the Bank. The arrangements shall provide the Bank with sufficient supervisory visibility to verify the amount, currency, location, accessibility and encumbrance status of the Operational Liquidity.

11.3.6 Concentration and diversification: Not more than fifty per cent (50%) of required Operational Liquidity shall be maintained with or dependent upon any single bank, custodian, liquidity provider or other counterparty. Operational Liquidity shall be maintained through not fewer than two (2) independent approved institutions. The Bank may prescribe lower concentration limits or additional diversification requirements based on to the scale, risk profile, systemic importance, cross-border arrangements or counterparty exposures of the Class 2 Licensed Issuer.

11.3.7 Supervisory confirmation: The Bank shall require direct confirmation from any deposit money bank holding or providing Operational Liquidity and may require such institution to provide balance confirmations, transaction information, account statements or other information reasonably necessary to verify compliance with this Section.

11.3.8 Replenishment: Where Operational Liquidity falls below the amount required under Section 11.3.1, the issuer shall rectify the non-compliance within three (3) business days of its occurrence or such shorter period as the Bank may prescribe. The Bank may restrict new issuance, distribution, customer acquisition, transaction volumes or other activities until the deficiency has been remedied.

11.3.9 Stress-testing methodology: The stress-testing methodology under Section 11.3.1(c) shall be approved or prescribed by the Bank and shall be sufficiently conservative to assess the ability of the issuer to meet Nigerian redemption and payment obligations during severe but plausible stress.

The methodology shall take into account, at a minimum:

a) historical Nigerian redemption outflows;

b) the largest observed redemption periods over the preceding prescribed by the Bank;

c) redemption concentrations over one-day, five-day and thirty-day periods;

d) market-price dislocation or depegging scenarios;

e) disruption or unavailability of banking, custody, settlement or payment infrastructure;

f) counterparty concentration and failure;

g) impairment or delay of cross-border access to liquidity;

h) foreign-exchange market stress;

i) weekends, public holidays and settlement-system outages; and

j) such other severe but plausible scenarios as the Bank may prescribe.

The Bank shall require a higher Operational Liquidity amount where the results of stress testing demonstrate that the amounts calculated under Section 11.3.1(a) or (b) would be insufficient.

11.3.10 Additional requirements: The Bank may prescribe higher Operational Liquidity requirements, additional buffers, eligible liquidity resources, concentration limits, stress-testing requirements, reporting obligations or liquidity-management standards having regard to the scale, value, volume, redemption profile, market conditions, foreign-exchange conditions, cross-border access risks, systemic importance or other risk characteristics of the Class 2 Stablecoin or issuer.

Operational liquidity maintained under this Section shall be additional to and separate from, and shall not be counted toward or reduce, the Reserve Pool, reserve-backing requirements, or required regulatory capital otherwise applicable under these Regulations.

11.3.11 Capital and reserve treatment: Operational Liquidity maintained under this Section or Section 24.50 shall be separate from and additional to the following requirements and shall not be used to satisfy any part thereof:

a) the issuer's required regulatory capital;

b) the Reserve Pool or the full reserve-backing requirement applicable to the Class 2 Stablecoin;

c) the two per cent (2%) overcollateralisation requirement under Section 24.4; or

d) any other liquidity or capital requirement under these Regulations, including Sections 17.6 and 24.12, unless expressly permitted by the Bank.

11.4 Class 2 Supervision: The Bank shall maintain issuer and service-provider entries in its public register and shall continuously assess each Class 2 Licensed Issuer's capital, reserves, liquidity, redemption performance, governance arrangements, operational controls, Nigerian activities and compliance with these Regulations.

Each issuer shall maintain a standing regulatory contact in Nigeria and provide such periodic reports, data and information as the Bank may require, including information relating to circulation, transaction volumes and values, reserve assets, liquidity, redemption activity, operational incidents and cross-border arrangements.

11.5 Distribution Controls: A Class 2 Stablecoin shall be distributed only through persons licensed or authorised by the Bank under these Regulations.

Each approved distributor or service provider shall:

a) conduct KYC, AML/CFT/CPF and sanctions-screening measures in accordance with applicable law;

b) comply with applicable Travel Rule requirements;

c) support approved redemption arrangements;

d) maintain records and submit reports required by the Bank; and

e) comply with any conditions imposed by the Bank relating to foreign-exchange management, payment-system integrity or financial stability.

11.6 Data Access and Regulatory Controls: Each Class 2 Licensed Issuer and its approved service providers shall provide the Bank with such information and transaction-level data as may be lawfully required.

A Class 2 Stablecoin shall incorporate such controls as the Bank may require to facilitate compliance with applicable law and lawful regulatory directions, including controls relating to transaction monitoring, freezing, blocking, burning or other regulatory interventions.

11.7 Monetary and Foreign-exchange Safeguards: The Bank may impose restrictions, limits, reporting requirements, reserve-backing requirements, operational-liquidity requirements, circulation thresholds, transaction caps, customer eligibility conditions or other safeguards on a Class 2 Stablecoin where necessary to support monetary policy implementation, financial stability, payment-system integrity, consumer protection or foreign-exchange management.

11.8 Redemption rights and local arrangements:

Each Class 2 Licensed Issuer shall:

a) provide holders with clear, legally enforceable redemption rights in accordance with these Regulations;

b) maintain approved Nigerian redemption arrangements capable of processing redemption requests within the required timeframe;

c) identify and maintain any approved distribution, banking, custody and redemption partners required by the Bank; and

d) maintain such technical, operational, governance and cooperation arrangements as are necessary to support effective supervision and compliance with lawful directions of the Bank.

11.9 Applicability of Other Requirements: A Class 2 Licensed Issuer shall comply with all issuer licensing, incorporation, governance, capital, reserve, liquidity, operational resilience, independent assessment and supervisory-access requirements applicable under these Regulations, including those contained in Sections 7, 14, 15, 17 and 24.

11.10 Cross-border payments: This Section applies to every Cross-Border Virtual Asset Transaction carried out, facilitated or settled by a Licensee, a person authorised under these Regulations, an Authorised Dealer, an International Money Transfer Operator or a payment service provider licensed by the Bank. It supplements, and does not displace, the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act 1995, the Foreign Exchange Manual and other directives of the Bank on foreign exchange (together, the "FX Regulations").

11.10.1 A Cross-Border Virtual Asset Transaction is any transfer, payment, settlement, conversion or redemption involving a Regulated Token or other virtual asset where:

a) the originator and the beneficiary are resident in different jurisdictions;

b) value is transferred between a Licensee and a VASP, financial institution or other person outside Nigeria;

c) value is transferred from a Licensee to an Unhosted Wallet, unless the Licensee has verified under Section 26.14 that the wallet is controlled by its customer or by another person resident in Nigeria;

d) it discharges, settles or prefunds an obligation between a person resident in Nigeria and a person resident outside Nigeria; or

e) it involves conversion between Naira and a Class 2 Stablecoin or other foreign-currency value for the purpose of a transaction in paragraphs (a) to (d).

Residence shall be determined in accordance with the FX Regulations.

11.10.2 For the purposes of the FX Regulations, a Cross-Border Virtual Asset Transaction shall be treated as a foreign-exchange transaction of the corresponding current-account or capital-account category. It shall be subject to the same eligibility, documentation, reporting and settlement requirements as the equivalent transaction in foreign currency.

11.10.3 A Licensee shall not carry out a Cross-Border Virtual Asset Transaction on documentation, verification or reporting less than would be required for the equivalent transaction through an Authorised Dealer.

11.10.4 A Licensee may carry out a Cross-Border Virtual Asset Transaction only where:

a) the transaction falls within the scope and conditions of its approval to conduct cross-border activity under Section 9.14; and

b) the underlying purpose is permitted under the FX Regulations.

11.10.5 a) A payment for imported goods made in a Class 2 Stablecoin shall be supported by a valid Form M. A payment for imported services shall be supported by the documentation required under the FX Regulations. The Licensee shall record the reference in the transaction record and pay only the foreign supplier or its VASP.

b) Where export proceeds are received in a Class 2 Stablecoin, the relevant Form NXP shall be referenced. The proceeds shall be treated as repatriated only when redeemed or converted and credited to the exporter's export-proceeds domiciliary account with an Authorised Dealer within the period prescribed by the FX Regulations. Holding the export proceeds on-chain in a wallet, in Nigeria or elsewhere, shall not constitute repatriation.

c) The Licensee shall provide the Authorised Dealer that processed the Form M or Form NXP with the transaction details needed to close the relevant record.

11.10.6 a) An inbound personal remittance using a virtual asset shall be provided only by an International Money Transfer Operator licensed by the Bank, or by a Licensee approved under Section 9.1 acting with such an operator.

b) The beneficiary shall be paid in Naira, or in such other currency as the Bank determines, through the operator's designated Naira settlement account, in accordance with the IMTO Regulations.

c) An outbound personal transfer by an individual shall count towards the eligible allowance under the FX Regulations.

11.10.7 a) A capital inflow received in a virtual asset shall not qualify for an electronic Certificate of Capital Importation unless, and until, it is converted into Naira through an Authorised Dealer in accordance with the FX Regulations. The Licensee shall disclose this to the customer before the transaction.

b) The acquisition of virtual assets outside Nigeria by a resident, and any borrowing, lending or capital contribution in a Class 2 Stablecoin between a resident and a non-resident, shall be subject to the FX Regulations applicable to the equivalent capital-account transaction.

11.10.8 An Authorised Dealer, International Money Transfer Operator, payment service provider or Licensee shall not use a virtual asset to settle, prefund, net or otherwise discharge obligations to a foreign counterparty arising from a foreign-exchange or remittance transaction, except under an arrangement approved by the Bank for that purpose. Where the Bank permits aggregation or net settlement, each underlying transaction shall remain individually identifiable and shall be documented, classified and reported on a gross basis in accordance with the FX Regulations and these Regulations.

11.10.9 A Licensee shall carry out Cross-Border Virtual Asset Transactions only:

a) in corridors approved or permitted by the Bank;

b) with counterparties that are licensed or registered, and supervised for AML/CFT/CPF purposes, in their jurisdiction under Section 26.16; and

c) with originator and beneficiary information transmitted under Section 26.14 [irrespective of the value of the transfer].

11.10.10 The Bank may prescribe in Schedule 9 transaction and periodic limits by customer category and purpose.

11.10.11 Before each Cross-Border Virtual Asset Transaction, a Licensee shall disclose to the customer:

a) the total cost, including all fees;

b) the exchange rate applied and its margin over [the Nigerian Foreign Exchange Market reference rate];

c) the expected delivery time; and

d) the consequences under the FX Regulations, including those in Sections 11.10.5(b) and 11.10.7(a).

The Licensee shall also provide payment-status tracking.

11.10.12 In addition to Sections 20.9 and 20.10, a Licensee shall report:

a) each Cross-Border Virtual Asset Transaction, at the regulated gateway, within [one Business Day], stating the purpose code, the Form M, Form NXP or eCCI reference where applicable, the corridor, the counterparty VASP identifier, the wallet type, the fiat and token legs, and the rate; and

b) monthly aggregates by corridor, purpose, token and direction, in the form prescribed in Schedule 7, for foreign-exchange and balance-of-payments monitoring.

11.10.13 Each Class 2 Licensed Issuer and its distributors shall report quarterly the number and value of transactions in which a Class 2 Stablecoin is used as a means of exchange between persons in Nigeria. Where the level, value or pattern of such transactions meets such criteria or indicators as the Bank may prescribe, the Bank may restrict further issuance or distribution to persons in Nigeria under Section 11.7

11.10.14 Where necessary to address disorderly conditions in the foreign-exchange market, pressure on the balance of payments or external reserves, or large or disruptive capital movements, the Bank may, by direction to Licensees and Authorised Dealers, impose such measures as it considers necessary and proportionate, including to:

a) lower limits or extend holds;

b) suspend specific corridors, purposes, tokens or counterparties;

c) cap volumes, values or the onboarding of new customers;

d) require conversions and redemptions to be settled through an Authorised Dealer; or

e) suspend conversion between Naira and Class 2 Stablecoins.

11.10.15 No person shall structure, split or route a transaction, including through a P2P Service, an affiliate, an offshore entity or an Unhosted Wallet, to avoid this Section. A Licensee shall monitor for such conduct, report it to the Bank, and file a suspicious transaction report with the NFIU where required.

11.10.16 The Bank may approve, including within its Regulatory Sandbox, arrangements that interoperate with regional or bilateral payment infrastructure, on conditions it specifies. Admission to the Sandbox shall not constitute a licence.

11.10.17 Notwithstanding Sections 6.5 and 11.1, the Bank may recognise a foreign-currency-referenced stablecoin issued outside Nigeria. A Recognised Foreign Stablecoin may be used only by an Authorised Dealer or a Licensee expressly approved by the Bank for that purpose to settle wholesale Cross-Border Virtual Asset Transactions. Recognition requires that:

a) the issuer is licensed and supervised under a regime the Bank considers to deliver substantively equivalent outcomes;

b) the Bank has cooperation arrangements with the home authority;

c) redemption at par is legally enforceable by holders in Nigeria;

d) the issuer can freeze and block on lawful order; and

e) the stablecoin is not offered to retail customers in Nigeria.

Recognition may be varied or withdrawn at any time.

Part 5
Supervisory powers

Section 12 Authority Over Licensees

12.1 The Bank may conduct off-site and on-site supervision, examinations, inspections, system and control testing, reserve and redemption reviews, independent assessments, meetings with directors and senior management and validation of regulatory returns.

12.2 The Bank may require information, documents, records, data, explanations or access to relevant systems within a specified period for its supervisory, monetary policy, financial-stability, foreign-exchange, consumer-protection or enforcement functions. The entity shall ensure that records are complete, accurate, readily retrievable and reconcilable to relevant ledgers, blockchains, banks, custodians and other sources.

12.3 Where deficiencies or breaches arise, the Bank may issue a deficiency notice, require immediate remedial action or a time-bound action plan, require strengthened governance or controls, commission an independent review, restrict activities or new minting, require additional capital or liquidity, appoint a monitor or adviser at the entity's expense, or require a meeting of its board or shareholders.

12.4 The Bank may impose conditions on continued operations, require enhanced reporting, direct recovery or orderly wind-down and exercise suspension or revocation powers under Section 14. Administrative penalties shall remain subject to the applicable penalty provisions and their notice and representation procedures. No power in this section shall dispense with applicable statutory requirements for administration, asset transfers or insolvency.

12.5 The Bank shall coordinate with the SEC and other competent authorities where supervisory action affects an entity subject to their jurisdiction. Cooperation shall not diminish the entity's obligations to the Bank or prevent urgent action necessary within the Bank's lawful authority.

12.5 Risk-based supervision: The Bank shall supervise Licensees on a risk-sensitive basis, determining the frequency and intensity of on-site and off-site supervision by reference to the AML/CTF/CPF risk profile of each Licensee and of the sector. It shall maintain statistics on licensing, inspections, findings, sanctions and suspicious transaction reports, and shall issue guidance and feedback to Licensees, in coordination with the NFIU.

Section 13 Restrictions on Regulated Tokens and Services

13.1 An entity shall not conduct unapproved activities, deal in Prohibited Tokens or exceed its licence or authorisation. Algorithmic stablecoins without full reserve backing, the prohibited crypto-collateralised arrangements specified in these Guidelines, tokens issued by sanctioned entities or jurisdictions, and tokens designated unacceptable by the Bank shall remain prohibited.

13.2 Class 1 issuance shall be Naira-referenced. Class 2 issuance shall be foreign-currency-referenced and subject to approved use cases and foreign-exchange controls. A Platform-Facilitated Peer-to-Peer Service involving Class 2 Stablecoins against Naira is governed by Section 10, including the foreign-exchange and anti-circumvention requirements in Section 10.6.

13.3 An issuer shall not pay, offer, arrange or facilitate interest, yield, dividends, returns or other financial benefits to holders by reason of holding or depositing its stablecoin. A service provider shall not be used to circumvent this prohibition.

13.4 Reserves shall not be used for operating expenses, lending, staking, collateral for borrowing or other prohibited leverage or encumbrance. Customer assets shall not be used for a provider's own purposes. Any liquidity-management transaction expressly permitted by the Bank shall remain subject to the applicable reserve safeguards and shall not override an express prohibition elsewhere in these Guidelines.

13.5 No new tokens shall be minted unless equivalent Eligible Reserve Assets have been received. An issuer shall cease new issuance upon a reserve shortfall and comply with the applicable remediation and reporting requirements. Redemption shall remain available at par, within the prescribed period and without standard redemption charges, subject only to the exceptions expressly permitted by these Guidelines.

13.6 The Bank may impose limits on token circulation, transaction volume or value, customer numbers, new onboarding, distribution channels, conversion or admission to trading, or other activities where necessary for monetary stability, financial-system integrity or customer protection. The Bank may apply restrictions to an entity, token or category of regulated service.

13.7 An affected entity shall implement controls to comply with restrictions, promptly rectify breaches and provide daily compliance evidence where directed by the Bank. A restriction on new business shall not relieve an entity of outstanding redemption or customer-protection obligations.

13.8 No person shall represent a licence, authorisation or capital deposit as a guarantee by the Bank. Customer disclosures shall accurately state regulatory status, risks and applicable protections. Stablecoins shall not be represented as bank deposits or as covered by NDIC deposit insurance.

Section 14 Restrictions on Regulated Tokens and Services

14.1 **Suspension:** The Bank may suspend all or part of a licence or authorisation where there is persistent material non-compliance despite remediation, a material reserve shortfall not restored within the required period, inability to meet redemption or customer obligations, failure of the board or management to satisfy fit and proper requirements, a financial-crime investigation, the provision of false, misleading or incomplete information, the conduct of an activity outside the scope of the licence or authorisation, the suspension or loss of an underlying licence, or a need to protect customers, the payments system or financial stability.

14.2 The suspension notice shall state its scope, grounds, effective date and applicable conditions. Suspension may take immediate effect where the Bank considers immediate action necessary; otherwise it shall take effect on the date specified in the notice.

14.3 During suspension, the entity shall cease the suspended activities, new minting, new customer onboarding and new distribution. It shall safeguard customer and reserve assets, maintain records and reporting, cooperate with supervisory and law-enforcement processes and continue redemption and other protective activities unless otherwise directed by the Bank. Suspension shall not automatically suspend redemption.

14.4 The Bank shall lift a suspension when satisfied that its grounds have been remedied. A suspension continuing for more than ninety calendar days without remediation shall be reviewed for revocation; revocation shall not occur automatically on expiry of that period.

14.5 **Voluntary Withdrawal:** An entity proposing to surrender its licence or authorisation or cease or materially discontinue its regulated business shall notify the Bank in advance and submit its board-approved wind-down plan. It shall not treat surrender as effective until the Bank confirms withdrawal and the conditions for cessation. The plan shall provide for customer notices, cessation of new business, orderly redemption or return or approved transfer of customer assets, treatment of unclaimed proceeds, settlement of obligations and preservation of records.

14.6 **Revocation:** The Bank may revoke a licence or authorisation where suspension grounds persist beyond the remediation period; approval was obtained by fraud, misrepresentation or concealment; the entity has ceased the approved business for twelve continuous months or more; it, or any of its directors or controllers, has been convicted of a criminal offence in Nigeria or elsewhere of an offence involving fraud, dishonesty, money laundering, terrorist or proliferation financing, sanctions evasion or a contravention of financial-services law, or of any other offence which in the opinion of the Bank renders it unfit to hold a licence; it enters liquidation, insolvency or administration; its shareholders resolve to wind up; or revocation is necessary in the public interest.

14.7 Before revocation, the Bank shall give at least thirty (30) days' written notice and an opportunity to make representations, except where immediate revocation is necessary to protect consumers or the financial system. The Bank shall consider representations received and communicate its decision in writing.

14.8 Upon revocation, the Bank shall publish notice and direct an orderly cessation. For an issuer, the Bank shall appoint a Special Purpose Administrator to manage orderly redemption and the application of reserve assets for holders, in accordance with applicable law.

As a condition of its licence, every Licensed Issuer shall irrevocably consent to, and shall procure that its reserve custodians recognise, the appointment by the Bank of a Special Purpose Administrator to take control of the Reserve Pool and administer redemptions, to the extent permitted by law and without prejudice to any proceedings under the Companies and Allied Matters Act, 2020. For other providers, the Bank may direct the safeguarding, return or transfer of customer assets and the completion or orderly termination of outstanding transactions.

14.9 Withdrawal, suspension or revocation shall not discharge accrued obligations, including redemption, customer protection, reporting, cooperation and record retention. An entity shall not release capital or distribute reserve or customer assets to shareholders contrary to outstanding holder claims, applicable law or the Bank's directions.

14.10 Where an SEC-licensed entity is affected, the Bank shall coordinate with the SEC concerning the consequences for the entity and its customers. A CBN decision under this section shall address the CBN licence or authorisation; the SEC shall determine action concerning its own licence under applicable law.

14.11 **Loss of Underlying Licence:** An Other Services Authorisation or Approval to Extend Permitted Activities shall cease to have effect, to the extent it depends on an underlying licence, registration or approval, or part of it, that is suspended, revoked, expired or withdrawn, unless the Bank determines otherwise in writing. Sections 14.3, 14.8 and 14.9 shall apply, with necessary modifications to the orderly cessation of the affected activities.

14.12 The holder of an Other Services Authorisation or an Approval to Extend Permitted Activities shall notify the Bank immediately, and in any case not later than the next Business Day, upon the suspension, revocation, expiry or withdrawal of its underlying licence, registration or approval.

Part 6
Operational Requirements

Section 15 Capital Requirements for Class 1 and Class 2 Licensed Issuers

15.1 A Class 1 Licensed Issuer shall maintain paid-up capital of ten billion Naira (₦10,000,000,000), or such higher amount as the Bank may prescribe, on entry and at all times thereafter.

15.2 A Class 2 Licensed Issuer shall maintain minimum paid-up capital of fifteen billion Naira (₦15,000,000,000), or such higher amount as the Bank may prescribe, on entry and at all times thereafter.

15.3 Both classes shall comply with the capital deposit and corresponding evidence and supplementary requirements in Section 17. There is no offshore issuer exemption from incorporation, licensing or capital.

Section 16 Capital Requirements for Other Non-Security Virtual Asset Services

16.1 A provider of Other Non-Security Virtual Asset Services shall maintain minimum paid-up capital of one billion Naira (₦1,000,000,000), or such higher amount as the Bank may prescribe, on entry and at all times thereafter. Where it holds an SEC licence, this amount shall be additional to the capital set by the SEC for the relevant service type.

16.2 The capital requirement in Section 16.1 shall apply to the holder of an Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities under Section 9. The capital deposit and corresponding evidence and supplementary requirements in Section 17 shall apply. The CBN capital shall be distinct from and additional to capital presented to the SEC or any other regulatory authority for an operating licence. The same capital shall not be counted towards both requirements, and applicable capital under another principal licensing framework shall remain payable.

16.3 The holder of an Approval to Extend Permitted Activities shall continue to meet the capital requirements of its Principal Licence and shall, in addition, maintain the minimum paid-up capital required under Section 16.1 for Other Non-Security Virtual Asset Services. Capital maintained to satisfy the requirements of the Principal Licence shall not be counted towards the requirement under Section 16.1. The Bank may require higher capital or additional liquidity in accordance with Section 17.4 having regard to the nature, scale and risk of the approved activities.

Section 17 Supplementary Capital Liquidity and Systemic Requirements

17.1 Required capital shall consist of cash in the designated capital account at the Bank or Federal Government of Nigeria securities held with a custodian approved by the Bank and subject to a lien in favour of the Bank. Additional capital under Section 15 shall be held in assets approved by the Bank. RTGS evidence for cash deposits shall identify the remitting institution, remitter, amount, value date, transaction reference and designated account, together with source-of-funds information and confirmation of receipt. For permitted securities, provide custody and lien evidence satisfactory to the Bank. Except for securities expressly permitted by this Section, non-cash contributions, virtual assets, guarantees and anticipated transfers shall not qualify.

17.2 Capital held at the Bank, or subject to the Bank's lien, under Section 17.1 shall remain so held. It shall not be withdrawn, pledged, charged or otherwise encumbered without the Bank's prior written approval. No release shall reduce eligible capital below the applicable requirement or prejudice outstanding obligations. Capital compliance shall include both the prescribed paid-up capital and the required capital deposit; a deposit shall not excuse the erosion of paid-up capital by losses.

17.3 Capital shall be separate from and additional to issuer reserves, the CBN reserve deposit, customer funds and assets and operational liquidity. No amount shall be counted simultaneously towards these separate requirements. Capital maintained to satisfy a Principal Licence, or capital presented to the SEC or any other regulatory authority for an operating licence, shall not also count towards the CBN capital requirement for Other Non-Security Virtual Asset Services.

17.4 The Bank may require a Non-Security Virtual Asset Issuer to maintain higher capital where its scale, activities or risk profile warrant an increase in the applicable capital requirement, taking into account transaction volumes, market significance, redemption obligations, operational and technology risks, concentration, interconnectedness, and the nature and complexity of its business.

The Bank may require higher capital based on the value of a Regulated Tokens in circulation, transaction volumes, systemic significance, redemption obligations, operational and technology risks, concentration, interconnectedness, and the nature and complexity of the business. Systemic designation shall not reduce any capital requirement or displace enhanced reserve, liquidity, reporting, stress-testing or recovery requirements under these Guidelines

The Bank may require higher capital having regard to circulation, transaction volumes, systemic significance, redemption obligations, operational and technology risks, concentration, interconnectedness and the nature and complexity of the business. Systemic designation shall not reduce any capital requirement or displace enhanced reserve, liquidity, reporting, stress-testing or recovery requirements under these Guidelines.

17.5 An entity that falls below its capital requirement shall notify the Bank immediately and submit a capital restoration plan within ten Business Days. The Bank may restrict new issuance, onboarding or other activities until capital is restored and may take further supervisory action. The Bank may review and revise capital requirements by circular.

17.6 Licensed Issuers shall maintain, from own funds and separately from the Reserve Pool, liquid assets sufficient to cover the higher of (a) six months of projected operating expenses; and (b) the cost of orderly wind-down set out in the approved wind-down plan. Reserve liquidity for redemptions shall be governed by Sections 23 and 24. The required capital deposit shall not be treated as freely available operating or redemption liquidity. Operational Liquidity maintained by a Class 2 Licensed Issuer under Sections 11 and 24.50 shall not count towards this requirement.

Systemic Stablecoins

17.7 Licensed Issuers shall maintain, from own funds and separately from the Reserve Pool, liquid assets sufficient to cover the higher of (a) six months of projected operating expenses; and (b) the cost of orderly wind-down set out in the approved wind-down plan. Reserve liquidity for redemptions shall be governed by Sections 23 and 24. The required capital deposit shall not be treated as freely available operating or redemption liquidity. Operational Liquidity maintained by a Class 2 Licensed Issuer under Sections 11 and 24.50 shall not count towards this requirement.

17.8 A Licensed Issuer of a Systemic Stablecoin shall maintain the capital floor under Section 15 and any higher capital prescribed by the Bank, provide continuous real-time reserve reporting, conduct stress testing at least twice yearly and maintain an approved recovery and resolution plan. Class 1 reserve-deposit requirements in Section 24 and Class 2 operational-liquidity requirements in Sections 11 and 24.50 apply according to the issuer's class.

17.9 The Bank may impose further enhanced requirements on a Systemic Stablecoin having regard to its nature, size, interconnectedness and criticality.

Section 18 Assessment of Shareholders Controllers Directors and Senior Management

18.1 Before granting a licence or authorisation, the Bank shall assess the fitness and propriety of directors, senior management, controllers and significant shareholders holding five per cent or more of issued share capital. Ownership shall be disclosed through to ultimate beneficial owners, including indirect holdings and persons exercising control other than through share ownership.

17.5 An entity that falls below its capital requirement shall notify the Bank immediately and submit a capital restoration plan within ten Business Days. The Bank may restrict new issuance, onboarding or other activities until capital is restored and may take further supervisory action. The Bank may review and revise capital requirements by circular.

17.6 Licensed Issuers shall maintain, from own funds and separately from the Reserve Pool, liquid assets sufficient to cover the higher of (a) six months of projected operating expenses; and (b) the cost of orderly wind-down set out in the approved wind-down plan. Reserve liquidity for redemptions shall be governed by Sections 23 and 24. The required capital deposit shall not be treated as freely available operating or redemption liquidity. Operational Liquidity maintained by a Class 2 Licensed Issuer under Sections 11 and 24.50 shall not count towards this requirement.

Systemic Stablecoins

17.7 Licensed Issuers shall maintain, from own funds and separately from the Reserve Pool, liquid assets sufficient to cover the higher of (a) six months of projected operating expenses; and (b) the cost of orderly wind-down set out in the approved wind-down plan. Reserve liquidity for redemptions shall be governed by Sections 23 and 24. The required capital deposit shall not be treated as freely available operating or redemption liquidity. Operational Liquidity maintained by a Class 2 Licensed Issuer under Sections 11 and 24.50 shall not count towards this requirement.

17.8 A Licensed Issuer of a Systemic Stablecoin shall maintain the capital floor under Section 15 and any higher capital prescribed by the Bank, provide continuous real-time reserve reporting, conduct stress testing at least twice yearly and maintain an approved recovery and resolution plan. Class 1 reserve-deposit requirements in Section 24 and Class 2 operational-liquidity requirements in Sections 11 and 24.50 apply according to the issuer's class.

17.9 The Bank may impose further enhanced requirements on a Systemic Stablecoin having regard to its nature, size, interconnectedness and criticality.

Section 18 Assessment of Shareholders Controllers Directors and Senior Management

18.1 Before granting a licence or authorisation, the Bank shall assess the fitness and propriety of directors, senior management, controllers and significant shareholders holding five per cent or more of issued share capital. Ownership shall be disclosed through to ultimate beneficial owners, including indirect holdings and persons exercising control other than through share ownership.

18.2 No person shall become a controller, significant shareholder, director or member of senior management without the Bank's prior written approval. Changes in ownership, beneficial ownership or control shall be disclosed before implementation and shall be subject to applicable prior approval. The Bank may impose conditions on an approved acquisition or exercise of control where necessary to address supervisory concerns.

18.3 Assessment shall cover:

a) integrity, including convictions involving dishonesty, fraud, financial crime or moral turpitude; adverse regulatory or professional findings; and involvement in institutional failure or mismanagement reflecting adversely on suitability;

b) competence, including qualifications, relevant experience, knowledge and capacity appropriate to the proposed role;

c) financial soundness, including insolvency, bankruptcy proceedings within the preceding ten years and unsatisfied court judgments arising from financial obligations; and

d) independence and conflicts of interest, including whether independent non-executive directors can exercise independent judgment.

18.4 The Bank may conduct background and reference checks and require police clearance certificates, credit reports, source-of-wealth and source-of-funds evidence and other relevant information. Approval shall be subject to continuing fitness and propriety. An entity shall promptly notify the Bank of information affecting an approved person's suitability.

18.5 Subject to applicable legal prohibitions and the Bank's prior approval where an exception is lawfully available, the following shall not participate in ownership, control or a significant beneficial interest: serving staff of regulated financial service providers; governments at any level; public officers within the applicable constitutional definition; sanctioned persons or entities; serving staff of financial regulatory or supervisory agencies; persons convicted of financial crimes; insolvent or bankrupt persons; persons failing fit and proper requirements; shell companies or entities with opaque ownership; and other persons designated by the Bank. Approval shall not override a statutory prohibition or sanctions restriction.

18.6 A person of significant control associated with a licensed or authorised VASP shall not acquire control of another licensed or authorised VASP without prior regulatory approval.

18.7 Banks and financial holding companies may participate in VASP ownership only through a separately incorporated subsidiary and with the prior approval of the Bank. This shall not prevent a Deposit Money Bank licensed by the Bank from undertaking Non-Security Virtual Asset Payment Activities under an Approval to Extend Permitted Activities. It does not permit a deposit money bank or financial holding company to issue a stablecoin otherwise than through a Class 1 or Class 2 Licensed Issuer that is a separately incorporated subsidiary. A bank's issuance of Deposit Money Tokens remains governed by Part 10. No issuer shall be controlled by a person or related group prohibited from financial-institution management under BOFIA 2020 or subject to criminal proceedings for financial crime in any jurisdiction.

18.8 Other service providers shall maintain governance appropriate to their services and applicable principal licensing framework, together with any additional conditions imposed by the Bank. The Bank may withdraw approval of a director or senior manager who ceases to satisfy the criteria. The entity shall replace that person within sixty days of notification and comply with any interim restrictions or protective directions.

Section 19 Principal Business

19.1 A Class 1 Licensed Issuer's principal and exclusive regulated business shall be the approved issuance and redemption of its Naira-referenced token and activities integral to that function, including token generation, minting, distribution on its own behalf, maintenance of associated technology, reserve management and burning.

19.2 A Class 2 Licensed Issuer's principal and exclusive regulated business shall be the approved issuance and redemption of its foreign-currency-referenced token and activities integral to that function. It shall maintain the Nigerian substance, approved reserve and redemption arrangements and foreign-exchange controls required by these Guidelines Regulations.

19.3 An issuer shall not conduct an unrelated commercial or financial business or provide separate third-party non-issuance services merely by virtue of its Issuer Licence. Any proposed additional Regulated Activity shall require the Bank's prior written approval and any separate licence or authorisation required by law. Integral activities outsourced to another person shall be performed on the issuer's behalf under compliant outsourcing arrangements, and the issuer shall remain responsible.

19.4 The principal business of the holder of an Other Services Licence shall be the services specified in its licence. The business of the holder of an Other Services Authorisation may comprise its SEC-approved activities and the Non-Security Virtual Asset services expressly authorised by the Bank. A financial institution licensed by the Bank shall retain the limitations of its Principal Licence and shall obtain an Approval to Extend Permitted Activities under Section 9.6, or such other licence or authorisation as is required under Section 9, for the proposed Non-Security Virtual Asset services.

19.5 An entity conducting more than one approved service shall maintain identifiable records, responsibilities, financial information, customer assets and controls for each service, manage conflicts and prevent contagion between activities. Ancillary business shall remain within its approved scope. No entity shall undertake securities-related or other separately regulated business without the relevant competent authority's approval.

Section 20 Notification Reporting and Annual Compliance Requirements

20.1 **Application Changes:** An applicant, licensee or authorised entity shall immediately notify the Bank of material changes affecting the accuracy or completeness of application information and supply the relevant documents. Notification shall not replace any requirement for prior approval.

20.2 **Reporting Calendar:** The returns, frequencies and deadlines applicable to Licensed Issuers and other Licensees are set out in the Reporting Calendar in Schedule 7, which shall prevail over any inconsistent timeline elsewhere in these Regulations. Returns shall be submitted in the electronic format prescribed by the Bank.

20.3 Reportable events Each regulated entity shall report material incidents or changes affecting or reasonably likely to affect compliance, capital, reserves, redemption, customer assets, governance, cybersecurity or operational continuity. Events include cyberattacks, unauthorised access, data breaches, smart contract vulnerabilities, critical outages, reserve shortfalls, loss of access to assets, redemption delays, material de-pegging, failure of a critical provider, ownership or management changes, control failures, insolvency proceedings material legal, regulatory, disciplinary or enforcement action in Nigeria or abroad, including any such action, licence refusal, suspension or revocation concerning agroup entity that provides virtual asset services in any jurisdiction.". Relevant changes in external regulatory requirements shall also be reported.

20.4 **Timing:** Reportable incidents shall be notified in writing within twenty-four hours of awareness. An imminent or serious threat to holders, reserves, redemption or operational continuity, an acute stress event, a capital shortfall or another event expressly requiring immediate reporting shall be reported immediately. Foreseeable material changes shall be notified before implementation within the period prescribed by the Bank and be subject to applicable prior approval; unforeseen material changes shall be notified as soon as practicable after awareness.

20.5 **Follow-up:** Within seventy-two hours of the initial incident notification, the entity shall submit a detailed report stating the event's nature, timing, cause and impact; affected systems, services and assets; actual or potential consequences; containment and recovery measures; remediation; and prevention of recurrence. Information not yet established shall be identified and updated. Stress-event reporting shall continue at the frequency directed by the Bank until discontinued by the Bank.

20.6 **Independent Obligations:** An issuer and its distribution, custody, exchange, wallet or other service provider shall each report events affecting its own obligations. A report by one party shall not discharge another's independent duty. Notification to the Bank shall not replace suspicious transaction reports or other reports required to the NFIU or another competent authority.

20.7 Reserve assurance Each Licensed Issuer shall publish, and submit to the Bank, a monthly reserve attestation by an Approved Independent Auditor, prepared under ISAE 3000 (Revised) or an equivalent standard approved by the Bank, within fifteen Business Days of month-end, in the form in Schedule 6, covering circulation, reserve value and composition, segregation, concentration, the CBN reserve deposit where applicable and Class 2 operational liquidity and compliance with reserve backing. Annual audited financial statements, including a separate opinion on reserve management, shall be submitted within four months of financial year-end.

20.8 **Periodic Operational Returns:** Each licensee or authorised entity shall submit returns in the forms and at the frequencies prescribed by the Bank, covering its activities, volumes and values, token circulation where applicable, customer exposures, assets held, capital, liquidity, reserves, reconciliation exceptions, redemption performance, complaints, operational incidents, AML/CFT/CPF controls and compliance with restrictions. Complaints registers shall form part of quarterly regulatory reporting.

20.9 **Class 2 Returns:** A provider distributing or facilitating Class 2 Stablecoins shall submit monthly transaction reports within ten Business Days after month-end unless otherwise prescribed, including volumes and values, Naira inflows and outflows, aggregated user demographics and suspicious patterns. It shall submit quarterly reports on the top ten counterparties by transaction volume for Nigerian-originating or Nigerian-receiving transactions and immediate reports of material changes in the issuer's reserves, regulatory status or operational capability. Class 2 Licensed Issuers shall supply corresponding issuer-level information required by the Bank.

20.10 **Foreign-exchange Monitoring:** Cross-border Class 2 transactions shall be reported at the regulated gateway or other designated reporting point. Returns involving conversion between Naira and foreign-currency value shall identify the fiat and token legs, conversion rate, transaction purpose, direction of flow and counterparty category, together with other information prescribed for foreign-exchange and balance-of-payments monitoring.

20.11 **P2P Reporting:** A provider operating a Platform-Facilitated Peer-to-Peer Service shall comply with the AML/CFT/CPF, record-keeping and reporting requirements of Section 10.7 and Section 10.8.

20.12 **Annual Declaration:** Each issuer shall submit an annual renewal declaration by 31 January confirming continuing compliance, certified by its Chief Executive Officer and Chief Compliance Officer, with the prescribed fee, current reserve attestation, summary of material incidents, complaints and regulatory actions and financial statements required for renewal. Where the immediately preceding year's audit is not yet due under Section 20.7, the latest audited financial statements and current management accounts shall accompany the declaration, followed by that year's audited statements within the four-month deadline. Other providers shall comply with the renewal and annual compliance conditions specified in their licence or authorisation. Persistent failure following a deficiency notice may result in suspension.

20.13 **Other Continuing Notifications:** Issuers shall maintain daily reserve reconciliation records; submit independent penetration-test results within thirty days of completion; obtain the approvals required for material custody or governance changes; and disclose material changes to published customer information within forty-eight hours. The separate incident, redemption-suspension, wind-down, systemic and other reporting requirements of these Regulations shall continue to apply.

20.14 **Data Quality and Supervisory Access:** Returns shall be complete, accurate, timely and reconcilable to underlying records. The Bank may require corrections, independent validation, more frequent or real-time reporting and additional periodic or ad hoc information. Outsourcing, offshore storage or group confidentiality arrangements shall not prevent lawful supervisory access. Failure to provide required information shall constitute a compliance breach.

Section 21 Use of Agents and Distributors

21.1 Before appointing an agent or distributor to perform a regulated service on its behalf, a licensee or authorised entity shall assess the arrangement and obtain any approval required by the Bank. The submission shall identify the agent, ownership, management, service scope, locations, customer interactions, operational capacity, fitness and propriety, AML/CFT/CPF controls, asset safeguards, technology and contractual arrangements.

21.2 No agent shall conduct an activity requiring a separate licence in its own right without that licence. Appointment as an agent shall not confer issuer status or permit distribution of an unapproved token. An issuer shall undertake the distributor due diligence and written allocation of responsibilities required by Section 26.

21.3 The principal shall remain responsible for the regulated service, monitor the agent, ensure appropriate training and qualifications, maintain records and access rights, and require the agent to disclose to customers the principal on whose behalf it acts. Customer complaints and asset protection shall remain subject to these Regulations.

21.4 Material changes, control failures and termination affecting an agency arrangement shall be notified under Section 20. The Bank may require further information, impose conditions or direct suspension or termination where the arrangement presents unacceptable risk. The principal shall ensure continuity and orderly return or transfer of customer assets.

Section 22 Outsourcing

22.1 A regulated entity shall maintain a board-approved outsourcing policy and assess the risks of material outsourced functions before engagement or material change. It shall obtain prior approval where required by the Bank and provide details of the provider, services, location, ownership, subcontracting, controls, access and exit arrangements.

22.2 A written agreement shall specify responsibilities, service and security standards, confidentiality and data protection, business continuity, incident reporting, audit rights, access to systems and records for the entity and competent authorities, subcontracting controls and orderly termination or transfer.

22.3 Outsourcing shall not transfer regulatory responsibility, impair supervision, obscure customer asset ownership, frustrate lawful directions or prevent records from being produced in Nigeria without delay. The entity shall exercise continuing oversight, test contingency arrangements and manage concentration and cross-border risks.

22.4 An outsourcing provider shall not perform an activity for which a separate licence or authorisation is required without obtaining it. Reliance on a third party for CDD is distinct from outsourcing and shall comply with Section 26.

Section 23 Issuance and Redemption of Stablecoins

23.1 No issuer shall mint stablecoins against anticipated receipts. Equivalent Eligible Reserve Assets shall have been received before minting. Issuance and redemption shall be subject to CDD and sanctions requirements in Section 26 and the continuous reserve and reconciliation requirements in Section 24.

23.2 Every holder of a Stablecoin issued by a Licensed Issuer under these Regulations shall have an absolute, legally enforceable right to redeem their stablecoin tokens at par value at any time, subject only to the exceptions expressly provided in these Regulations.

23.3 Every Licensed Issuer shall maintain operational systems and sufficient reserve liquidity to redeem its stablecoins at par, in the reference currency, no later than the end of the Business Day following the day on which a valid redemption request is received. Where a Stress Event occurs, the Bank may, on application, permit redemption within such longer period as it specifies, not exceeding five Business Days or any shorter maximum prescribed by law.

23.4 No Licensed Issuer shall charge a fee for a standard redemption. The Bank may approve a fee that is proportionate to, and does not exceed, the actual cost incurred for a redemption requiring non-standard settlement, provided it is disclosed in the Whitepaper and customer agreement. No minimum redemption amount shall exceed such amount as the Bank may prescribe.

23.5 A Licensed Issuer may suspend redemption operations only in the following circumstances:

a) pursuant to a court order from a court of competent jurisdiction;

b) pursuant to a written directive from the Bank;

c) where there is a documented, material technical failure of the issuer's platform or the underlying blockchain network that prevents the processing of redemption transactions, provided that such technical failure shall be notified to the Bank immediately and the issuer shall take all practicable steps to restore redemption capability within twenty-four (24) hours; or

c) where the Bank has designated the stablecoin as a Systemic Stablecoin and issues an instruction suspending redemption as a financial stability measure.

23.6 An issuer that suspends redemptions shall notify the Bank immediately and in any case within one hour, and shall not continue the suspension beyond forty-eight hours without the Bank's written approval.

23.7 Where redemption is suspended for any reason, the Licensed Issuer shall immediately:

a) notify the Bank in writing;

b) publish a public notice disclosing the reasons for suspension and the expected restoration timeline; and

c) continue to process pending redemption requests upon restoration of redemption capability, in the order in which they were received.

23.6 The issuer shall maintain a clear minting, transfer, redemption and burning lifecycle, reconcile redeemed tokens to reserve outflows and outstanding circulation, and prevent redeemed tokens from remaining available for re-use. Any intermediary redemption route shall preserve the issuer's responsibility for the holder's enforceable redemption right.

Section 24 Management and Safekeeping of the Reserve Pool

Requirement for Reserves

24.1 Every Licensed Issuer shall maintain at all times a Reserve Pool whose value in the reference currency equals or exceeds the par value of all its stablecoin obligations. Full backing and the additional buffer under Section 24.4 shall be maintained continuously, not merely at periodic reporting dates. Class 2 records and returns shall also state the Naira equivalent under the Bank's prescribed valuation methodology.

24.2 Every Licensed Issuer shall ensure that the Reserve Pool fully backs all Stablecoins in issuance at all times on a one-to-one basis. For the purposes of this requirement, Stablecoins in issuance shall include Stablecoins in circulation as well as Stablecoins that have been redeemed but have not yet been permanently removed from circulation, burned or otherwise extinguished.

24.3 No Licensed Issuer shall issue new stablecoin tokens (mint) unless, at the time of minting, equivalent Eligible Reserve Assets have been received and held in the Reserve Pool. Minting against anticipated future reserve receipts is prohibited.

24.4 A Licensed Issuer shall maintain overcollateralisation of not less than two per cent (2%) of the par value of stablecoins in circulation, to absorb valuation losses on reserve assets and accrued operational liabilities. The buffer shall not be released without the prior approval of the Bank.

Daily Reconciliation and Shortfall Management

24.5 Every Licensed Issuer shall, at the end of each Business Day, reconcile the total number and aggregate value of Stablecoins in circulation against the value and composition of the Reserve Pool maintained in accordance with these Regulations.

24.5.1 Temporary deviations from the Class 1 Reserve Deposit requirement under Section

24.25 may occur because of significant redemptions, liquidity stress or exceptional circumstances. A Class 1 Licensed Issuer shall restore compliance as soon as practicable and comply with the notification and remediation requirements below. This provision shall not excuse a shortfall in full reserve backing.

24.5.2 A Class 1 Licensed Issuer shall notify the Bank on the same Business Day where the balance in its Reserve Deposit Account falls below the twenty per cent (20%) of the Reserve Pool as required under Section 24.25. Where the shortfall continues for more than five consecutive Business Days, the issuer shall cease new issuance until compliance is restored and shall submit a restoration plan under Section 24.5.3.

The notification shall include the reasons for the shortfall, the amount and duration of the shortfall, and the remedial measures being undertaken to restore compliance.

24.5.3 Following a notification under Section 24.5.2, the issuer shall submit a remediation and restoration plan detailing the actions and timeline for restoring compliance with the Class 1 Reserve Deposit requirement. The Bank may impose additional conditions or supervisory measures where considered necessary.

24.6 The reconciliation under Section 24.5 shall identify, at a minimum:

a) the total number of Stablecoins in circulation;

b) the aggregate value of the Reserve Pool, determined in accordance with the valuation methodology prescribed by the Bank;

c) the balance of each reserve account and the location and composition of the Reserve Assets;

d) all issuances, redemptions, reserve movements and material valuation adjustments occurring during the relevant period; and

e) any discrepancy between outstanding Stablecoins and the Reserve Pool.

24.7 A Licensed Issuer shall notify the Bank immediately, and in any event within twenty-four (24) hours of becoming aware of the occurrence, of any reserve shortfall, material reconciliation discrepancy or failure to access Reserve Assets when required to meet redemption obligations.

24.8 Where a reserve shortfall occurs, the Issuer shall immediately cease issuing new Stablecoins and shall notify the Bank of the nature and extent of the shortfall, its cause, the corrective measures proposed and the anticipated time for remediation.

24.9 The Issuer shall not resume issuance until the shortfall has been fully remedied and the Bank has been notified of the remediation, subject to any further direction issued by the Bank.

24.10 The Issuer shall maintain records of each daily reconciliation and make such records available to the Bank and its Independent Auditor upon request.

24.11 The Bank may prescribe additional reconciliation requirements, including more frequent or real-time reconciliation, having regard to the size, nature, complexity and risk profile of the Issuer.

Liquidity Management and Reserve Maturity

24.12 Every Licensed Issuer shall maintain not less than forty per cent (40%) of its total Reserve Pool in cash or Eligible Reserve Assets qualifying as HQLA. For Class 1, this minimum is in addition to the CBN Reserve Deposit, which shall not count towards it. A Class 2 issuer shall meet this reserve-liquidity minimum in the reference currency and separately maintain operational liquidity under Sections 11 and 24.50, which shall not count towards this minimum; no fixed domestic reserve share is imposed. Non-cash assets counted shall have residual maturity not exceeding six months and satisfy any shorter category-specific limit. A board-approved liquidity policy shall ensure timely conversion into funds to meet foreseeable redemptions.

24.13 The policy shall address, at a minimum:

a) the minimum level of immediately available cash and cash-equivalent reserve assets to be maintained;

b) the maturity profile of reserve assets and the concentration of assets maturing on any particular date;

c) projected and actual redemption demands, including periods of unusually high or concentrated redemptions;

d) the time required to liquidate or realise each category of reserve asset without material loss;

e) the availability of liquidity during weekends, public holidays, banking disruptions and settlement-system outages; and

f) contingency arrangements for the failure or unavailability of a reserve bank, custodian or other material service provider.

24.14 The issuer shall establish and document a reserve maturity profile appropriate to the denomination, liquidity characteristics and redemption obligations of the stablecoin. It shall identify the cash and high-quality liquid assets counted towards the forty per cent (40%) minimum, the residual maturity of each non-cash asset and compliance with the six-month ceiling and any shorter category-specific limit. A demand cash deposit has no fixed residual maturity.

24.15 The Bank may prescribe minimum liquidity thresholds, maturity limits, liquidity coverage requirements or other prudential measures, having regard to the nature and risk profile of the Stablecoin and the Issuer's redemption history.

24.16 The Issuer shall review the liquidity management policy at least annually and following any material change in its reserve composition, redemption profile or operational arrangements.

Stress Events and Supervisory Intervention

24.17 For the purposes of these Regulations, a "Stress Event" means an event or circumstance that has occurred or is reasonably likely to occur and that materially impairs, or threatens to impair, the ability of a Licensed Issuer to maintain reserve backing, provide timely redemption, safeguard Reserve Assets or continue critical issuance and redemption operations.

24.18 A Stress Event includes:

a) a material reserve shortfall or failure of daily reserve reconciliation;

b) an unusual or concentrated increase in redemption requests that threatens the Issuer's ability to meet its obligations when due;

c) persistent failure to process or settle valid redemption requests within the period prescribed under Section 23;

d) a material deviation of the market price of the Stablecoin from its reference value;

e) the insolvency, suspension, loss of authorisation or material operational failure of a reserve bank, custodian or other critical service provider;

f) a material disruption affecting the issuance, transfer or redemption of the Stablecoin; or

f) any other event designated by the Bank as a Stress Event.

24.19 A Stablecoin Issuer shall notify the Bank immediately for an acute stress event, upon becoming aware that a stress event has occurred or is reasonably likely to occur.

24.20 The notification shall state the nature and commencement of the event, the amount of stablecoins outstanding, the status and liquidity of the Reserve Pool, the volume of pending redemption requests, the measures already taken and the further measures proposed.

24.21 Upon the occurrence of a Stress Event, the Issuer shall activate its contingency arrangements and comply with any direction issued by the Bank, including directions to:

a) increase immediately available liquidity;

b) cease or restrict new issuance;

c) submit daily or more frequent reserve and redemption reports;

d) liquidate or transfer specified Reserve Assets, subject to the requirements of these Regulations;

e) take corrective action within a specified period; or

e) implement an orderly redemption or wind-down plan.

24.22 A Licensed Issuer shall submit periodic updates to the Bank for the duration of a stress event and shall not discontinue enhanced reporting until the Bank is satisfied that the event has been resolved or directs otherwise.

24.23 The Bank may prescribe quantitative triggers, reporting intervals, liquidity requirements and other measures applicable to particular classes of Stablecoin or categories of issuer.

24.24 Nothing in this Section authorises suspension of redemption except on the grounds in Section 23.5 and subject to Sections 23.6 and 23.7 and any lawful direction of the Bank.

Stress Events and Supervisory Intervention

24.25 Every Class 1 Licensed Issuer shall maintain not less than twenty per cent (20%) of its total Reserve Pool as a cash deposit at the Bank in a dedicated Reserve Deposit Account. This requirement shall not apply to Class 2 Licensed Issuers, whose operational liquidity is governed by Sections 11 and 24.50.

24.26 The CBN Reserve Deposit shall be established by agreement between the Class 1 Licensed Issuer and the Bank in the form prescribed in Schedule 4 and shall be subject to the following conditions:

a) the deposit shall be maintained at the Bank and may not be withdrawn without the Bank's prior written consent;

b) the Bank shall maintain real-time visibility into the balance of the Reserve Deposit Account;

c) the Reserve Deposit shall not bear interest; and

d) the Reserve Deposit shall ordinarily serve as a backstop in a significant redemption stress event and shall be accessed only after the issuer has exhausted its operational liquidity buffer, immediately available commercial-bank cash, and other readily liquid reserve assets, unless the Bank directs otherwise for financial stability reasons.

24.27 The Bank may, by directive, adjust the Class 1 CBN Reserve Deposit percentage for monetary policy and financial stability, provided it shall not fall below twenty per cent (20%) of the total Reserve Pool.

Composition of Eligible Reserve Assets

24.28 For Class 1 Stablecoins, the following assets are designated as Eligible Reserve Assets. Their eligibility shall not, by itself, establish that they qualify for the cash and high-quality liquid asset minimum in Section 24.12. The six-month ceiling for assets counted towards that minimum and any shorter maturity limits below shall apply:

a) deposits at the Central Bank of Nigeria (constituting the CBN Reserve Deposit required under Section 24);

b) Nigerian Treasury Bills issued by the Federal Government of Nigeria with a residual maturity of not more than ninety (90) days;

c) Federal Government of Nigeria bonds with a residual maturity of not more than one hundred and eighty (180) days;

d) naira-denominated cash deposits held at CBN-licensed commercial banks in segregated reserve accounts;

e) units in naira-denominated money market funds regulated by the SEC, subject to a maximum allocation of ten percent (10%) of total reserves;

f) overnight reverse repurchase agreements with Deposit Money Banks collateralised by Federal Government of Nigeria securities, subject to such haircut and counterparty limits as the Bank may prescribe; and

g) Open Market Operation bills issued by the Bank with a residual maturity not exceeding ninety (90) days.

24.29 No Licensed Issuer shall issue new stablecoin tokens (mint) unless, at the time of minting, equivalent Eligible Reserve Assets have been received and held in the Reserve Pool. Minting against anticipated future reserve receipts is prohibited.

a) for a Class 1 Stablecoin, assets denominated in any currency other than the Naira;

b) equities or equity-linked instruments;

c) corporate bonds or commercial paper;

d) virtual assets, including cryptocurrencies, other stablecoins, or digital tokens;

e) loans or receivables;

f) physical commodities;

g) real property; and

h) any asset that is subject to a charge, lien, pledge, or other encumbrance.

24.30 Class 2 reserves. The Reserve Pool of a Class 2 Stablecoin shall be held in the reference currency and shall consist of

a) cash deposits with Deposit Money Banks or with foreign banks approved by the Bank;

b) sovereign securities of the reference-currency jurisdiction with a residual maturity not exceeding ninety-three (93) days; and

c) overnight reverse repurchase agreements collateralised by the securities in paragraph (b). The issuer shall maintain operational liquidity under Sections 11 and 24.50. No fixed proportion of the Class 2 Reserve Pool is required by these Regulations to be held in Nigeria.

Protection and Segregation of Reserve Assets

24.31 All reserve assets shall be held in accounts and structures that are:

a) legally and operationally segregated from the Licensed Issuer's own operational funds, corporate assets, and any other assets not constituting part of the Reserve Pool;

b) clearly identified in the records of the custodian as held exclusively for the benefit of stablecoin holders as a class; and

c) structured, whether by statutory trust, charge, or such other legally enforceable mechanism as the Bank may approve, to ensure that in the event of the insolvency or receivership of the Licensed Issuer, stablecoin holders have first priority claim on the Reserve Pool ahead of all other creditors of the issuer.

24.32 The Licensed Issuer shall obtain an independent legal opinion from counsel qualified under Nigerian law confirming the enforceability of the segregation and priority arrangements referred to in Section 24.31 and shall submit such opinion to the Bank as part of the licensing application and whenever material changes to the custody arrangements occur.

24.33 Reserve assets shall not be used for any purpose other than supporting redemption and permitted liquidity management. Except for a transaction expressly permitted under the following paragraph, no Licensed Issuer shall lend, pledge, hypothecate, stake or otherwise encumber reserve assets or expose them to any risk that could materially impair their availability for redemption. Investments shall be limited to the Eligible Reserve Assets permitted by this Section.

24.34 A regulated repurchase or other secured liquidity-management transaction may constitute a narrow exception to the prohibition on reserve encumbrance only where expressly approved or permitted by the Bank, is conducted against eligible high-quality liquid assets, does not create material leverage or compromise segregation or priority, and remains subject to immediate unwind and redemption requirements prescribed by the Bank.

Protection and Segregation of Reserve Assets

24.35 No single CBN-licensed deposit money bank shall hold more than thirty per cent (30%) of the issuer's total Reserve Pool, measured by reserve value, whether as deposits or custodial assets. The denominator shall include the CBN Reserve Deposit. The CBN shall not be treated as a deposit money bank for this limit. For Class 2 reserves held with an approved foreign bank, the Bank may prescribe concentration limits under Section 24.39.

24.36 Where a Licensed Issuer's Reserve Pool is invested in Nigerian Treasury Bills or Federal Government bonds, no single counterparty (including any dealer, custodian, or sub-custodian) shall hold more than forty percent (40%) of such investment portfolio.

24.37 A Class 1 Licensed Issuer shall maintain reserves across not fewer than three distinct CBN-licensed Deposit Money Banks, in addition to the Reserve Deposit Account, subject to Section 24.35. A Class 2 issuer shall maintain diversified custody and banking arrangements approved under Sections 11 and 24.39, without a minimum domestic reserve share or a requirement to place reserves with three Nigerian banks.

24.38 A Deposit Money Bank shall be eligible to hold reserve deposits only if it holds a national or international banking licence, meets its prudential requirements and has not been subject to regulatory forbearance in the preceding twelve months.

24.39 The Bank may by directive impose additional concentration limits on specific Licensed Issuers where it determines that concentration risk poses a material threat to the safety of the Reserve Pool.

Prohibition on Leverage and Encumbrance

24.40 A Licensed Issuer shall not, except for a liquidity-management transaction expressly permitted by the Bank under this Section:

a) lend or otherwise advance any reserve asset to any person or entity;

b) pledge, charge, hypothecate, or otherwise encumber any reserve asset as security for any obligation of the issuer;

c) use reserve assets as collateral for borrowing;

c) invest reserve assets in any instrument other than the Eligible Reserve Assets specified in Section 24.

24.41 Any transaction in violation of Section 24.40 shall be treated in accordance with applicable law, including any applicable rule rendering it void, and the Licensed Issuer shall be subject to the enforcement measures prescribed in Part 11.

Reserve Attestations and External Audit

24.42 Every Licensed Issuer shall publish a reserve attestation report on a monthly basis, within fifteen (15) Business Days following the end of each calendar month, in accordance with Section 20.7.

24.43 Every Licensed Issuer shall publish a reserve attestation report on a monthly basis, within fifteen (15) Business Days following the end of each calendar month, in accordance with Section 20.7.

a) the total number of stablecoin tokens in circulation as of the attestation date;

b) the aggregate naira value of the Reserve Pool as at the attestation date;

c) the composition of the Reserve Pool by asset type, institution, and percentage allocation;

d) the balance and compliance status of the Class 1 CBN Reserve Deposit, or the adequacy and accessibility of Class 2 operational liquidity, as applicable;

e) confirmation that reserve assets are held in segregated accounts in compliance with Section 24.31;

f) confirmation that reserve concentration limits have been complied with;

g) any material changes to custody arrangements since the preceding attestation; and

h) the attestor's conclusion as to whether the reserve backing requirement has been satisfied.

24.44 Reserve attestation reports shall be submitted to the Bank. The prescribed format for reserve attestation reports is set out in Schedule 6.

24.45 Every Licensed Issuer shall submit annual audited financial statements to the Bank within four (4) months of the end of each financial year. The annual audit shall be conducted by an Approved Independent Auditor and shall include an opinion on the adequacy and integrity of the reserve management practices of the issuer.

Reserve Attestations and External Audit

24.46 Every Licensed Issuer shall hold the Reserve Pool on trust for the holders of its stablecoins under a declaration of trust in the form approved by the Bank, shall obtain and submit an independent legal opinion confirming that the Reserve Pool is bankruptcy-remote from the issuer's estate, and shall procure written acknowledgement of the trust from each reserve custodian. Subject to applicable insolvency law, the insolvency or receivership of a Licensed Issuer shall not affect the rights of stablecoin holders to the Reserve Pool, and holders shall have first-priority claims on the Reserve Pool as a class ahead of all other creditors of the issuer.

24.47 The Licensed Issuer shall ensure that trust and segregation arrangements under Sections 24.31 and 24.46 are structured to be enforceable under applicable insolvency law and supported by the independent legal opinion required by these Regulations. The Bank may require further agreements or safeguards within its lawful powers. These Regulations shall not themselves create a statutory trust or alter statutory insolvency priorities.

24.48 Where a Licensed Issuer becomes insolvent or is placed into receivership or administration, the Bank shall appoint a Special Purpose Administrator whose primary mandate shall be the orderly redemption of all outstanding stablecoins from the Reserve Pool and the return of any residual reserve assets to holders on a pro rata basis.

24.49 The Licensed Issuer shall, as a condition of its licence, maintain a wind-down plan approved by the Bank setting out the steps to be taken in the event of the orderly cessation of the issuer's operations, including the process for notifying holders, initiating mass redemption, and transferring or liquidating the Reserve Pool.

Class 2 Reserve and Redemption Arrangements

24.50 Each Class 2 Licensed Issuer shall appoint a Deposit Money Bank as a Nigerian redemption agent and maintain approved arrangements capable of meeting expected and stressed Nigerian redemption demand within the timeframes prescribed under Section 23. Operational liquidity shall be maintained in accordance with Section 11.3 and shall remain separate from the Reserve Pool and required regulatory capital. It shall not reduce or substitute for full reserve backing. The issuer shall maintain systems and controls sufficient to ensure that Operational Liquidity remains continuously available for Nigerian redemption and payment obligations and shall monitor compliance with the minimum requirement under Section 11.3.1 on an ongoing basis.

24.50.1 Monthly reporting: Each Class 2 Licensed Issuer shall submit to the Bank, not later than ten (10) Business Days after the end of each calendar month, a report setting out, at a minimum:

a) the total amount of Operational Liquidity maintained during and at the end of the reporting period;

b) the currency composition of the Operational Liquidity;

c) the location, account bank, custodian or other institution through which the Operational Liquidity is maintained;

d) the aggregate Nigeria-linked outstanding liabilities used for the calculation under Section 11.3.1(b);

e) the minimum Operational Liquidity required under each of Sections 11.3.1(a), (b) and (c), and the amount actually maintained;

f) Nigerian redemption requests and completed redemptions during the reporting period, including aggregate value, volume and average processing time;

g) the highest daily and weekly Nigerian redemption outflows during the reporting period;

h) any replenishment of Operational Liquidity during the reporting period;

i) any concentration exposure to a bank, custodian, liquidity provider or other counterparty;

j) the results of stress testing conducted during the reporting period or since the previous report; and

k) such other information as the Bank may prescribe.

24.50.2 Immediate notification: A Class 2 Licensed Issuer shall notify the Bank as soon as practicable and in any event within two (2) hours of becoming aware of any of the following events:

a) Operational Liquidity Shortfall:

   i) When Operational Liquidity has fallen below 100 per cent of the minimum amount required under Section 11.3.1; or

   ii) based on known redemption requests, payment obligations or other committed outflows, Operational Liquidity is reasonably projected to fall below the required minimum within the following five (5) Business Days.

b) Impairment of Access to Operational Liquidity:

   i) ten per cent (10%) or more of required Operational Liquidity becomes frozen, blocked, encumbered, unavailable for withdrawal or otherwise inaccessible;

ii) any restriction or delay prevents the issuer from accessing an amount necessary to satisfy redemption or payment obligations falling due during the following twenty-four (24) hours; or

iii) access to any material Operational Liquidity account, facility or custodian is interrupted for more than two (2) consecutive hours during a period in which Nigerian redemption or payment obligations are outstanding.

c) Material Depegging Event:

A material depegging event shall be deemed to occur where the market price of a Class 2 Stablecoin:

i) deviates by more than one per cent (1%) from its reference value for thirty (30) consecutive minutes, measured using a representative market-price methodology approved or prescribed by the Bank; or

ii) deviates by more than two per cent (2%) from its reference value at any time under that methodology. The issuer shall report the cause or suspected cause, affected markets, redemption conditions, Operational Liquidity position and remedial measures being taken.

d) Unusual or Concentrated Nigerian Redemption Activity:

A material increase in Nigerian redemption activity shall be deemed to occur where:

i) during any rolling twenty-four-hour period, Nigerian redemption requests equal or exceed five per cent (5%) of Nigeria-linked outstanding liabilities;

ii) during any rolling twenty-four-hour period, the value of Nigerian redemption requests exceeds two hundred per cent (200%) of the issuer's average daily Nigerian redemption requests during the preceding thirty (30) calendar days; or

iii) aggregate Nigerian redemption requests during any rolling seven-day period exceed ten per cent (10%) of Nigeria-linked outstanding liabilities.

e) Failure or Suspension of a Material Bank, Custodian, Redemption Agent or Settlement Provider:

The issuer shall notify the Bank where:

i) any bank, custodian, redemption agent, settlement provider or liquidity provider responsible for holding or providing ten per cent (10%) or more of required Operational Liquidity; or

i) any such provider processing twenty per cent (20%) or more of Nigerian redemption or settlement activity during the preceding thirty (30) calendar days, becomes insolvent, enters administration or resolution, has its licence or authorisation suspended or revoked, freezes or restricts the issuer's relevant accounts, ceases or materially restricts operations, or experiences an operational outage exceeding two (2) consecutive hours that materially affects Nigerian redemption or settlement capability.

Any insolvency, regulatory suspension or account freeze affecting a designated Nigerian redemption agent shall be reportable regardless of the quantitative thresholds above.

c) Actual or Anticipated Failure to Meet Redemption Obligations:

The issuer shall notify the Bank where:

i) any material category of valid Nigerian redemption requests is reasonably expected to exceed the redemption timeframe prescribed under Section 23;

ii) more than five per cent (5%) by value or number of valid Nigerian redemption requests received during any rolling twenty-four-hour period are not expected to be completed within the prescribed timeframe;

iii) a technology, banking, blockchain, custody, settlement or operational disruption persists for more than two (2) consecutive hours and materially affects the processing of Nigerian redemptions; or

iv) the issuer reasonably expects that it will be unable to satisfy Nigerian redemption or payment obligations as they fall due during the following twenty-four (24) hours.

24.50.3 Content of immediate notification: A notification under Section 24.50.2 shall, to the extent known at the time of notification, include:

a) the nature and time of the event;

b) the amount of Operational Liquidity required and actually available;

c) the value of Nigeria-linked outstanding liabilities;

d) the value and volume of pending Nigerian redemption requests;

e) the institutions, accounts, systems or blockchain networks affected;

f) the actual or potential impact on Nigerian customers;

g) the issuer's assessment of the likely duration of the event;

h) actions taken or proposed to restore compliance and protect Nigerian customers; and

i) such other information as the Bank may require.

An initial notification may be supplemented as additional information becomes available.

24.50.4 Enhanced reporting following a trigger event: Following an event under Section 24.50.2, the Bank may require the issuer to provide weekly, daily, intraday, real-time or near-real-time reporting until the Bank is satisfied that the event has been resolved.

Unless otherwise directed by the Bank, an issuer experiencing:

a) material depegging event;

b) a shortfall in required Operational Liquidity; or

c) Nigerian redemption requests exceeding ten per cent (10%) of Nigeria-linked outstanding liabilities during any rolling seven-day period, shall provide the Bank with a daily liquidity and redemption report until the relevant condition has ceased for at least five (5) consecutive Business Days.

24.50.5 Verification: The Bank may require independent verification, auditor confirmation, bank confirmation or other assurance regarding the amount, accessibility, currency composition, location, encumbrance status and legal status of Operational Liquidity.

24.50.6 No domestic reserve duplication: Nothing in this Section requires the entirety, or any fixed proportion, of the Class 2 Reserve Pool to be held in Nigeria. The Operational Liquidity requirement is an additional Nigerian liquidity safeguard intended to ensure the timely satisfaction of Nigerian redemption and payment obligations and shall not be construed as a substitute for, or duplication of, the full reserve-backing requirements applicable to the Class 2 Stablecoin.

24.50.7 Foreign-exchange settlement and capital-flow compliance: Notwithstanding the right of redemption at par in the reference currency under Section 23, the manner of settlement of a Class 2 Stablecoin redemption in Nigeria shall remain subject to applicable foreign-exchange laws, regulations, directives and approvals.

The Bank may require redemption proceeds attributable to persons in Nigeria to be:

a) settled through an Authorised Dealer;

b) converted into Naira through permitted foreign-exchange channels;

c) retained or credited in an eligible foreign-currency account;

d) supported by such documentation, purpose codes or reporting as the Bank may prescribe; or

e) otherwise settled in accordance with arrangements approved by the Bank. No redemption, payment, settlement or conversion arrangement involving a Class 2 Stablecoin shall be structured, routed or used to circumvent applicable foreign-exchange, capital-flow, documentation, reporting, payment-system or other regulatory requirements.

24.51 Section 24.28 applies to the Reserve Pool of a Class 1 Stablecoin and Section 24.30 to the Reserve Pool of a Class 2 Stablecoin. Section 24.29(b) to (h) applies to both classes. A licence condition shall not dispense with an express prohibition in this Section. A Class 2 applicant unable to demonstrate compliant backing and redemption arrangements shall not commence issuance.

24.52 The two per cent overcollateralisation requirement is additional to full par backing. Reserve coverage, applicable Class 1 CBN Reserve Deposit and Class 2 operational liquidity shall be valued consistently under the Bank's methodology, recording original denominations and Naira equivalents for Class 2 obligations. Class 2 operational liquidity shall not be counted as reserve backing or required capital, as provided in Section 11.3.11.

Section 25 Safeguarding Tokens and Customer Assets held for Custody and Transfer

25.1 A custodian, wallet provider or transfer provider controlling customer assets or credentials shall hold them separately from its own property and maintain records identifying each customer's entitlement. It shall reconcile asset holdings, customer balances and movements and investigate and report material discrepancies under Section 20.

25.2 The provider shall secure private keys and administrative access through effective access control, segregation of duties, recovery arrangements and audit trails. It shall not lend, pledge, stake, rehypothecate or use customer assets for its own purposes. An issuer's Reserve Pool shall remain subject to the separate segregation and holder-protection requirements in Section 24.

25.3 Customer terms shall explain custody, control, transfer and withdrawal arrangements, material subcustody or outsourced functions, fees, risks and the treatment of assets on the provider's failure. Contractual descriptions shall correspond to actual operational and legal arrangements.

25.4 The provider shall maintain an orderly return or approved transfer plan and preserve access to records and assets during disruption, suspension and wind-down. It shall not represent client assets as its own or apply them to its own creditors. The legal effect in insolvency shall remain subject to applicable law and enforceable safeguarding arrangements.

Part 7
AML/CFT/CPF Obligations

Section 26 Anti Money Laundering, Counter Terrorist Financing Counter Proliferation Financing and Sanctions

26.1 This Section applies to every Licensed Issuer to every holder of Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities, including a provider of a P2P Service (each a "VASP" for the purposes of this Part). A financial institution holding an Approval to Extend Permitted Activities shall continue to comply with the AML/CFT/CPF regulations applicable to it under its Principal Licence and shall, in addition, comply with Sections 26.14 to 26.16 and any other requirement of this Section specific to virtual assets. All controls shall be applied consistently with the MLPPA, TPPA, NFIU requirements and lawful sanctions directions.26.1 General Obligations and Risk Assessment

26.1.1 Every Licensed Issuer and licensed or authorised VASP shall comply with all obligations imposed on such institutions under MLPPA, TPPA, these Regulations and any directive, circular or guideline issued by the Bank.

26.1.2 Every Licensed Issuer and licensed or authorised VASP shall take appropriate steps to identify, assess and understand its money laundering, terrorist financing and proliferation financing risks, having regard to its customers, countries or geographic areas, products, services, transactions, delivery channels, counterparties, including VASPs outside Nigeria, P2P activity, unhosted wallets and decentralised arrangements, and the virtual assets and blockchain networks it issues or supports.

26.1.3 The risk assessment under 26.1.2 shall:

a) be documented;

b) consider all relevant risk factors, including the national risk assessment and any risk assessment, typology or guidance issued by the Bank or the NFIU, before determining the overall level of risk and the level and type of mitigation to be applied;

c) include an assessment of proliferation financing risk, being the risk of breach, non-implementation, or evasion of targeted financial sanctions relating to proliferation financing;

d) be reviewed at least annually and whenever there is a material change in the institution's business, products, technology, or risk environment; and

e) be provided to the Bank.

26.1.4 Every Licensed Issuer and licensed or authorised VASP shall identify and assess the AML/CFT/CPF risks that may arise from the development of new products, new business practices, new delivery mechanisms, and the use of new or developing technologies, including any new virtual asset, blockchain network, bridge, smart-contract function or Travel Rule solution. The assessment shall be completed and documented before the launch or use of the product, practice or technology, and the institution shall take appropriate measures to manage and mitigate the risks identified.

26.1.5 Every Licensed Issuer and licensed or authorised VASP shall:

a) have policies, controls and procedures, approved by its board of directors or senior management, that enable it to manage and mitigate the risks identified under 26.1.2 and those identified by the Bank, the NFIU or in the national risk assessment;

b) monitor the implementation of those policies, controls and procedures and enhance them where necessary; and

c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

26.1.6 A Licensed Issuer or licensed or authorised VASP may take simplified measures to manage and mitigate risks only where lower risks have been identified under 26.1.2 and the simplified measures are consistent with these Regulations. Simplified measures shall not be permitted where there is a suspicion of money laundering, terrorist financing, proliferation financing or sanctions evasion.

26.2 AML/CFT/CPF Compliance Programme

26.2.1 Every Licensed Issuer and licensed or authorised VASP shall implement a compliance programme which is proportionate to its AML/CFT/CPF risks and the size of its business, and which shall include:

a) a written AML/CFT/CPF policy approved by the board of directors and reviewed at least annually;

b) the risk assessment required under Section 26.1;

c) compliance management arrangements, including the appointment of a Chief Compliance Officer at management level in accordance with 26.2.2;compliance management arrangements, including the appointment of a Chief Compliance Officer at management level in accordance with 26.2.2;

d) policies, procedures and controls for customer due diligence, ongoing monitoring, transaction and wallet monitoring, Travel Rule compliance, targeted financial sanctions, suspicious transaction reporting, record keeping and escalation;

e) screening procedures to ensure high standards when hiring employees and appointing directors, agents and persons performing outsourced compliance functions;

f) an ongoing employee training programme in accordance with 26.2.4; and

g) an independent audit function to test the compliance programme in accordance with 26.2.5.

26.2.2 The Chief Compliance Officer:

a) shall be a fit and proper person at management level with sufficient independence, authority and resources;

b) shall act as, or supervise, the compliance function responsible for receiving internal suspicion reports and filing reports with the NFIU;

c) shall have timely and unrestricted access to customer, transaction, wallet and other relevant information, and direct access to the board of directors; and

d) shall be the money laundering reporting officer for the purposes of the Money Laundering (Prevention and Prohibition) Act, 2022.

26.2.3 The compliance programme shall be documented and made available to the Bank.

26.2.4 Training under 26.2.1(f) shall be provided at onboarding and at least annually to directors, senior management, employees, agents and relevant outsourced personnel, and shall cover AML/CFT/CPF obligations, targeted financial sanctions, virtual asset and stablecoin typologies, Travel Rule requirements, suspicious transaction reporting and the prohibition on tipping off.

26.2.5 The independent audit function under 26.2.1(g) shall be carried out at least annually by internal audit or a qualified external party independent of the compliance function, and its findings and remediation actions shall be reported to the board of directors and submitted to the Bank within thirty (30) days of completion.

26.3 Customer Due Diligence

26.3.1 A Licensed Issuer or licensed or authorised VASP shall not open, keep or provide anonymous accounts, accounts in obviously fictitious names, anonymous wallets, or any facility that prevents the identification and verification of the customer.

26.3.2 Every Licensed Issuer and licensed or authorised VASP shall undertake customer due diligence (CDD) measures:

a) when establishing a business relationship, and before permitting a customer to mint, purchase, hold, transfer or receive stablecoins or other virtual assets through its platform;

b) when carrying out an occasional transaction, including a virtual asset transfer, with a value equal to or above USD/EUR 1,000 or its naira equivalent, whether conducted as a single operation or in several operations that appear to be linked;

c) when there is a suspicion of money laundering, terrorist financing, proliferation financing or sanctions evasion, regardless of any exemption or threshold; and

d) when it has doubts about the veracity or adequacy of previously obtained customer identification data.

26.3.3 CDD measures shall include:

a) identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information;

b) verifying that any person purporting to act on behalf of the customer is so authorised, and identifying and verifying the identity of that person;

c) identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source, such that the Licensed Issuer or licensed or authorised VASP is satisfied that it knows who the beneficial owner is;

d) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

e) assigning and documenting a risk classification of low, medium or high to each customer.

26.3.4 For a customer who is a natural person, the Licensed Issuer or licensed or authorised VASP shall obtain and verify at a minimum:

a) full legal name, date of birth and nationality;

b) residential address;

c) a valid government-issued identity document, such as an international passport, driver's licence or permanent voter's card;

d) the National Identification Number (NIN) and, where the customer holds one, the Bank Verification Number (BVN); and for a foreign national without a NIN or BVN, an equivalent identifier; and

e) the source of funds and, where appropriate, the source of wealth.

e) risk-based blockchain analysis of relevant wallet histories, including identifying exposure to illicit or high-risk wallet addresses and assessing the origin and destination of funds, particularly where funds are received from multiple unrelated wallets.

26.3.5 For a customer that is a legal person or legal arrangement, the Licensed Issuer or licensed or authorised VASP shall understand the nature of the customer's business and its ownership and control structure, and shall identify the customer and verify its identity through:

a) its name, legal form and proof of existence;

b) the powers that regulate and bind it, and the names of the relevant persons holding senior management positions; and

c) the address of its registered office and, if different, its principal place of business.

26.3.6 For a legal person, the Licensed Issuer or licensed or authorised VASP shall identify the beneficial owner and take reasonable measures to verify the identity of:

a) the natural person who ultimately has a controlling ownership interest in the legal person;

b) to the extent there is doubt under (a) as to whether the person with the controlling ownership interest is the beneficial owner, or where no natural person exerts control through ownership interests, the natural person exercising control of the legal person through other means; and

c) where no natural person is identified under (a) or (b), the natural person who holds the position of senior managing official.

Where the legal person operates or uses a virtual asset wallet, or conducts transactions that are inconsistent with its declared business activities or business profile, the Licensed Issuer or licensed or authorised VASP shall undertake enhanced verification of the identity of the beneficial owner and the ownership and control structure of the legal person.

26.3.7 For a legal arrangement, the Licensed Issuer or licensed or authorised VASP shall identify and take reasonable measures to verify the identity of:

a) for a trust, the settlor, the trustee, the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership; and

b) for other types of legal arrangement, persons in equivalent or similar positions.

26.3.8 Every Licensed Issuer and licensed or authorised VASP shall conduct ongoing due diligence on the business relationship, including:

a) scrutinising transactions and wallet activity throughout the relationship to ensure that they are consistent with its knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds; and

b) ensuring that documents, data and information collected under the CDD process are kept up to date and relevant by reviewing existing records, particularly for higher-risk customers, at intervals determined by risk and at least every one year for high-risk customers and every three years for other customers.

26.3.9 A Licensed Issuer or licensed or authorised VASP shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting an occasional transaction. It may complete verification after establishing the business relationship only where:

a) this occurs as soon as reasonably practicable;

b) this is essential not to interrupt the normal conduct of business;

c) the AML/CFT/CPF risks are effectively managed; and

d) it has adopted risk management procedures, including limits on the number, type and amount of transactions, and does not permit any withdrawal, transfer to an external wallet or redemption until verification is completed.

26.3.10 Every Licensed Issuer and licensed or authorised VASP shall apply CDD requirements to existing customers on the basis of materiality and risk, and shall conduct due diligence on existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

26.3.11 Every Licensed Issuer and licensed or authorised VASP shall apply enhanced due diligence (EDD), proportionate to the risks, where higher AML/CFT/CPF risks are identified, including in relation to:

a) politically exposed persons, their family members and close associates, in accordance with Section 26.4;

b) customers, transactions and counterparties connected with countries referred to in Section 26.6:

c) customers whose transactions are inconsistent with their stated source of funds or business profile, or which are complex, unusually large or follow an unusual pattern with no apparent economic or lawful purpose;

d) legal persons or arrangements with complex ownership structures, nominee shareholders or bearer shares;

e) customers with significant exposure to unhosted wallets, as determined by the institution's risk assessment and any guidance issued by the Bank;

f) transactions involving mixers, tumblers, privacy-enhancing coins or other anonymity-enhancing technologies, or high-risk counterparty VASPs; and

g) any other higher-risk factor identified by the institution or prescribed by the Bank.

26.3.12 EDD measures shall include, as appropriate: obtaining additional information on the customer, beneficial owner and intended nature of the relationship; establishing the source of funds and source of wealth; obtaining senior management approval to commence or continue the relationship; conducting enhanced monitoring through more frequent reviews and more controls; and analysing the transaction path using blockchain analytics.

26.3.13 A Licensed Issuer or licensed or authorised VASP may apply simplified due diligence only in accordance with 26.1.6, including for customers onboarded through a tiered KYC framework approved by the Bank. Simplified measures shall be commensurate with the lower-risk factors and shall not apply where there is a suspicion of AML/CFT/CPF or sanctions evasion, or where specific higher-risk scenarios apply. Any reliance on another institution for CDD information shall comply with Section 26.5.

26.3.14 Where a Licensed Issuer or licensed or authorised VASP is unable to comply with the relevant CDD measures, it shall not open the account, commence the business relationship or perform the transaction, or shall terminate the business relationship, and shall consider filing a suspicious transaction report with the NFIU in relation to the customer.

26.3.15 Where a Licensed Issuer or licensed or authorised VASP forms a suspicion of AML/CFT/CPF or sanctions evasion and reasonably believes that performing the CDD process will tip off the customer, it shall not pursue the CDD process and shall instead file a suspicious transaction report with the NFIU.

26.4 Politically Exposed Persons

26.4.1 Every Licensed Issuer and licensed or authorised VASP shall have appropriate risk management systems to determine whether a customer, beneficial owner or person acting on behalf of a customer is a politically exposed person, a family member or a close associate of a politically exposed person. Such determination shall be made at onboarding, on an ongoing basis, and whenever there is a material change in customer information or activity.

26.4.2 In relation to a foreign politically exposed person, a Licensed Issuer or licensed or authorised VASP shall, in addition to the measures in Section 26.3:

a) obtain senior management approval before establishing or, for existing customers, continuing the business relationship;

b) take reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as foreign politically exposed persons; and

c) conduct enhanced ongoing monitoring of the business relationship.

26.4.3 In relation to a domestic politically exposed person or a person who is or has been entrusted with a prominent function by an international organisation, a Licensed Issuer or licensed or authorised VASP shall take reasonable measures to determine whether a customer or beneficial owner is such a person and, in cases of a higher-risk business relationship, shall apply the measures in 26.4.2(a) to (c).

26.4.4 The requirements in 26.4.1 to 26.4.3 shall apply to family members and close associates of all types of politically exposed persons.

26.4.5 A Licensed Issuer or licensed or authorised VASP shall document the basis for identifying a politically exposed person, the risk classification assigned, the approvals obtained, the enhanced measures applied, and any decision to continue, restrict or terminate the relationship.

26.5 Reliance on Third Parties

26.5.1 A Licensed Issuer or licensed or authorised VASP may rely on a third party to perform the CDD measures in 26.3.3(a) to (d) or to introduce business, provided that the conditions in this section are met. Ultimate responsibility for the CDD measures shall remain with the Licensed Issuer or licensed or authorised VASP relying on the third party.

26.5.2 A Licensed Issuer or licensed or authorised VASP relying on a third party shall:

a) immediately obtain from the third party the necessary information concerning the CDD measures in 26.3.3(a) to (d);

b) take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available by the third party upon request without delay; and

c) satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Section 26.3 and Section 26.12.

26.5.3 When determining in which countries a third party that meets the conditions may be based, a Licensed Issuer or licensed or authorised VASP shall have regard to information available on the level of country risk, and shall not rely on a third party based in a country referred to in 26.6.1.

26.5.4 Where a Licensed Issuer or licensed or authorised VASP relies on a third party that is part of the same financial group, the requirements of 26.5.2 and 26.5.3 may be treated as met where:

a) the group applies CDD, record-keeping and AML/CFT/CPF programme requirements in line with these Regulations;

b) the implementation of those requirements is supervised at group level by a competent authority; and

c) any higher country risk is adequately mitigated by the group's AML/CFT/CPF policies.

26.5.5 This section does not apply to outsourcing or agency relationships. Where a Licensed Issuer or licensed or authorised VASP outsources any CDD or other AML/CFT/CPF function, the outsourced provider shall be treated as part of the institution, which shall remain fully responsible for compliance and shall ensure that the Bank and the NFIU have access to the relevant information and records.

26.6 Higher-Risk Countries

26.6.1 Every Licensed Issuer and licensed or authorised VASP shall apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons, financial institutions and VASPs from countries for which this is called for by the FATF.

26.6.2 Every Licensed Issuer and licensed or authorised VASP shall apply countermeasures, proportionate to the risks, when called upon to do so by the FATF, and independently of any call by the FATF when directed by the Bank. Countermeasures may include:

a) enhanced reporting or systematic reporting of transactions;

b) limiting business relationships or transactions with the country or persons in it;

c) prohibiting reliance on third parties located in the country;

d) reviewing, amending or, if necessary, terminating counterparty VASP or distributor relationships in the country; and

e) any other measure prescribed by the Bank.

26.6.3 For countries under FATF increased monitoring, every Licensed Issuer and licensed or authorised VASP shall take the FATF's findings into account in its risk assessment and apply enhanced measures where the risks warrant.

26.6.4 The Bank shall publish or communicate to Licensed Issuers and licensed or authorised VASPs, by circular or otherwise, the countries referred to in this section and concerns about weaknesses in the AML/CFT/CPF systems of other countries.

26.7 Transaction and Wallet Monitoring

26.7.1 Every Licensed Issuer and licensed or authorised VASP shall deploy and maintain an automated transaction monitoring system, supported by blockchain analytics, configured to detect and generate alerts for:

a) transactions exceeding thresholds prescribed by the Bank or set in its risk assessment;

b) transactions involving wallet addresses on its deny-list, on any sanctions list referred to in Section 26.8, or associated with illicit activity;

c) transactions consistent with known virtual asset and stablecoin typologies, including structuring to avoid reporting thresholds, rapid layering through multiple wallets, suspicious or anomalous peer-to-peer patterns, including activity structured to evade applicable controls or reporting requirements, and mixing or tumbling;

d) transactions originating from or directed to countries referred to in Section 26.6;

e) large-value or rapid-succession transactions inconsistent with the customer's profile;

f) cross-chain bridging or chain-hopping activity that may obscure the origin or destination of funds; and

g) any other pattern or indicator prescribed by the Bank or the NFIU.

h) activity indicating that a customer is a VASP or is providing virtual asset services to third parties without disclosure, including volumes, frequency or numbers of counterparties inconsistent with retail use, pooled or omnibus flows, or links to platforms not licensed in Nigeria;

26.7.2 Each alert shall be reviewed and its disposition documented within five (5) Business Days, or within twenty-four (24) hours where the alert indicates a possible sanctions match or terrorist financing.

26.7.3 The monitoring system shall be calibrated and tested at least annually, and whenever there is a material change in the institution's products, customers or risk environment, to ensure that alerts reflect its current risks.

26.7.4 Where a customer appears to be acting as an undisclosed VASP, the Licensed Issuer or licensed or authorised VASP shall apply Section 26.16, restrict or terminate the relationship where the customer is not licensed or registered as required, file a suspicious transaction report where appropriate, and inform the Bank.

26.8 Targeted Financial Sanctions

26.8.1 Every Licensed Issuer and licensed or authorised VASP shall screen its customers, beneficial owners, persons acting on behalf of customers, counterparties and wallet addresses, at onboarding, before processing each transaction and whenever the lists are updated, against:

a) the United Nations Security Council Consolidated List; and

b) the Nigeria Sanctions List.

26.8.2 Where a Licensed Issuer or licensed or authorised VASP identifies virtual assets or other funds owned or controlled, wholly or jointly, directly or indirectly, by a designated person, or by a person acting on behalf of or at the direction of a designated person, it shall without delay and without prior notice:

a) freeze the virtual assets or funds;

b) not make any virtual assets, funds or financial or related services available, directly or indirectly, to or for the benefit of the designated person; and

c) report to the Nigeria Sanctions Committee and the NFIU the assets frozen and actions taken, including any attempted transactions.

26.8.3 The obligations in 26.8.1 and 26.8.2 apply to targeted financial sanctions relating to terrorism and terrorist financing and to the financing of proliferation of weapons of mass destruction.

26.8.4 Every Licensed Issuer and licensed or authorised VASP shall, as part of its risk management and having regard to its correspondent relationships, stablecoin infrastructure and cross-border exposure, assess whether to screen against other sanctions lists, including the OFAC Specially Designated Nationals List, the European Union Consolidated List and the United Kingdom Consolidated List, and shall document that assessment. A match against such a list shall trigger enhanced due diligence and a documented decision, which may include refusing or terminating the relationship or transaction and filing a suspicious transaction report.

26.8.5 Every Licensed Issuer and licensed or authorised VASP shall maintain procedures for:

a) promptly resolving potential matches, including false positives, before releasing any held transaction;

b) unfreezing assets upon delisting, or upon instruction of the competent authority where a person is confirmed not to be a designated person; and

c) giving effect to authorisations from the competent authority for access to frozen assets for basic or extraordinary expenses.

26.8.6 Every Licensed Issuer and licensed or authorised VASP shall subscribe to updates of the lists in 26.8.1 and implement them without delay.

26.9 Suspicious Transaction Reporting

26.9.1 Where a Licensed Issuer or licensed or authorised VASP suspects, or has reasonable grounds to suspect, that funds, virtual assets, a transaction, an attempted transaction or any wallet activity are the proceeds of criminal activity or unlawful activity as defined in the MLPPA, or are related to terrorist financing, proliferation financing or sanctions evasion, it shall report its suspicion to the NFIU promptly, and in any case within twenty-four (24) hours of forming the suspicion.

26.9.2 The obligation in 26.9.1 applies regardless of the amount involved, and whether the transaction was completed, attempted, rejected, suspended or abandoned.

26.9.3 A report under 26.9.1 shall be filed in the form and through the channel prescribed by the NFIU, and shall include all relevant information available to the institution, including customer and beneficial ownership information, wallet addresses, transaction hashes, counterparty VASP details, the grounds for suspicion and any action taken.

26.9.4 After filing a report, the Licensed Issuer or licensed or authorised VASP shall take appropriate risk-based action, including enhanced monitoring, and shall comply with any directive of the NFIU or other competent authority made under the MLPPA, including any instruction to postpone or stop a transaction.

26.9.5 A Licensed Issuer or licensed or authorised VASP shall respond promptly to any request by the NFIU for additional information relating to a report.

26.9.6 Every employee, agent and officer of a Licensed Issuer or licensed or authorised VASP shall report any knowledge or suspicion under 26.9.1 to the Chief Compliance Officer without delay.

26.10 Tipping Off, Confidentiality and Protection for Reporting

26.10.1 A Licensed Issuer or licensed or authorised VASP and its directors, officers, employees and agents shall be protected from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the NFIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

26.10.2 A Licensed Issuer or licensed or authorised VASP and its directors, officers, employees and agents shall not disclose to the customer or any other person the fact that a suspicious transaction report or related information is being, or has been, filed with the NFIU, or that an analysis or investigation is being carried out.

26.10.3 Nothing in 26.10.2 prohibits disclosure:

a) to the Bank, the NFIU or any other competent authority;

b) within the institution or its financial group for AML/CFT/CPF purposes in accordance with Section 26.13; or

c) as otherwise required or permitted by law.

26.10.4 Every Licensed Issuer and licensed or authorised VASP shall restrict access to information relating to suspicious transaction reports to authorised personnel and shall keep such information confidential.

26.11 Other Reporting Obligations

26.11.1 Every Licensed Issuer and licensed or authorised VASP shall submit to the NFIU, and to the Bank where prescribed, reports of:

a) cash and other transactions equal to or exceeding the thresholds prescribed under the MLPPA; and

b) transfers of funds or virtual assets to or from a foreign country equal to or exceeding the thresholds prescribed under the MLPPA or by the NFIU,

within the time and in the form prescribed.

26.11.2 For the purposes of section 26.11.1, virtual assets shall be valued at the time of the transaction in Naira or the applicable foreign currency, as the case may be. Transactions that appear to be linked or structured to avoid an applicable reporting threshold shall be reported individually and aggregated for the purpose of determining whether the reporting threshold has been met.

26.11.3 Every Licensed Issuer and licensed or authorised VASP shall submit such periodic returns on AML/CFT/CPF compliance, including returns on business relationships with politically exposed persons, as the Bank or the NFIU may prescribe.

26.11.4 Reports under this section are in addition to, and do not replace, the obligation to file a suspicious transaction report under Section 26.9.

26.12 Record Keeping

26.12.1 Every Licensed Issuer and licensed or authorised VASP shall maintain all necessary records on transactions, both domestic and international, for at least five (5) years after the completion of the transaction, in a manner sufficient to permit the reconstruction of individual transactions, including where applicable the amount and type of virtual asset, date and time, wallet addresses, transaction hashes, counterparty VASP, required information under Section 26.14, mint and redemption records, and exchange rates applied, so as to provide, if necessary, evidence for prosecution of criminal activity.

26.12.2 Every Licensed Issuer and licensed or authorised VASP shall keep all records obtained through CDD measures, account files and business correspondence, and the results of any analysis undertaken, including inquiries to establish the background and purpose of complex or unusual transactions, for at least five (5) years after the business relationship is ended or after the date of the occasional transaction.

26.12.3 Every Licensed Issuer and licensed or authorised VASP shall keep records of risk assessments, monitoring alerts and their disposition, sanctions screening results, internal suspicion reports, decisions on whether to file a report, reports filed with the NFIU, and freezing actions, for at least five (5) years.

26.12.4 Records shall be kept securely, protected against unauthorised access, alteration or loss, and shall be made available swiftly to the Bank, the NFIU and other competent authorities upon appropriate authority. Where records are held electronically, outside Nigeria or by an outsourced provider, the Licensed Issuer or licensed or authorised VASP shall remain responsible for ensuring that they can be produced in Nigeria without delay.

26.12.5 A Licensed Issuer or licensed or authorised VASP shall not destroy records that are the subject of a request, investigation, court order or supervisory direction, even after the retention period has expired, until it is notified that they are no longer required.

26.13 Group-Wide Programmes, Foreign Branches and Subsidiaries

26.13.1 A Licensed Issuer or licensed or authorised VASP that is part of a financial group shall implement group-wide AML/CFT/CPF programmes, applicable to all branches and majority-owned subsidiaries, which include the measures in Section 26.2 and:

a) policies and procedures for sharing information required for CDD and AML/CFT/CPF risk management;

b) the provision, at group-level compliance, audit and AML/CFT/CPF functions, of customer, account, wallet and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes, including information and analysis of unusual or suspicious transactions, and the receipt of such information by branches and subsidiaries when relevant to risk management; and

c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping off.

26.13.2 A Licensed Issuer or licensed or authorised VASP shall ensure that its foreign branches and majority-owned subsidiaries apply AML/CFT/CPF measures consistent with these Guidelines where the requirements of the host country are less strict, to the extent permitted by host-country law.

26.13.3 Where the host country does not permit the proper implementation of measures consistent with these Regulations, the Licensed Issuer or licensed or authorised VASP shall apply appropriate additional measures to manage the AML/CFT/CPF risks and shall inform the Bank without delay. The Bank may impose additional supervisory measures, including directing the institution to close the branch or subsidiary.

26.14 Transfer of Virtual Assets and Payment Transparency (Travel Rule)

26.14.1 This section applies to every virtual asset transfer, domestic or cross-border, in which a licensed or authorised VASP acts as the originating, intermediary or beneficiary institution. It also applies to a Licensed Issuer to the extent provided in Section 26.22, and to any financial institution licensed by the Bank when it sends or receives a virtual asset transfer on behalf of a customer.

26.14.2 The Travel Rule requirements in this Section shall be applied consistently with applicable Nigerian law and the Bank's lawful directives, having regard to FATF Recommendation 16 as applied to virtual assets under Recommendation 15. Any later applicable enactment shall prevail to the extent required by law.

26.14.3 For a virtual asset transfer equal to or above USD/EUR 1,000 or its naira equivalent, the originating licensed or authorised VASP shall obtain and hold required and accurate originator information and required beneficiary information, comprising:

a) the name of the originator;

b) the originator's account number or wallet address used to process the transfer or, where there is no account, a unique transaction reference number that permits traceability;

c) the originator's address, or NIN or customer identification number, or date and place of birth, and, for a legal person, its Legal Entity Identifier where available;

d) the name of the beneficiary; and

e) the beneficiary's account number or wallet address used to process the transfer or, where there is no account, a unique transaction reference number that permits traceability.

26.14.4 For a virtual asset transfer below the threshold in 26.14.3, the originating licensed or authorised VASP shall obtain and hold the name of the originator and the beneficiary, and the wallet address or unique transaction reference number of each. This information need not be verified for accuracy unless there is a suspicion of AML/CFT/CPF or sanctions evasion, in which case it shall be verified.

26.14.5 The originating licensed or authorised VASP shall submit the information in 26.14.3 or 26.14.4 to the beneficiary VASP or financial institution immediately and securely, before or simultaneously with the transfer, and shall make it available on request to the Bank, the NFIU and other competent authorities.

26.14.6 The originating licensed or authorised VASP shall not execute a virtual asset transfer if it cannot comply with 26.14.3 to 26.14.5. The obligations in Sections 26.14.3 to 26.14.5 apply regardless of whether the jurisdiction of the counterparty VASP has implemented the Travel Rule.

26.14.7 The beneficiary licensed or authorised VASP shall obtain and hold required originator information and required and accurate beneficiary information, and shall make it available on request to the Bank, the NFIU and other competent authorities.

26.14.8 The beneficiary licensed or authorised VASP shall take reasonable measures, which may include post-event or real-time monitoring where feasible, to identify virtual asset transfers that lack required originator or required beneficiary information, and shall have risk-based policies and procedures for determining:

a) when to execute, reject, suspend or return a transfer lacking required information, including withholding the virtual assets from the customer's account pending receipt of the information; and

b) the appropriate follow-up action, including requesting missing information, restricting or terminating the relationship with the counterparty, and filing a suspicious transaction report.

26.14.9 An intermediary licensed or authorised VASP shall ensure that all originator and beneficiary information that accompanies a virtual asset transfer is retained with it. Where technical limitations prevent the information from accompanying a related transfer, the intermediary shall keep a record of all information received for at least five (5) years. The intermediary shall take reasonable measures to identify transfers lacking required information and apply risk-based policies equivalent to 26.14.8.

26.14.10 Where several individual virtual asset transfers from a single originator are bundled in a batch file, the batch file shall contain required and accurate originator information and full beneficiary information that is fully traceable within the beneficiary country, and the originating licensed or authorised VASP shall include the originator's account number, wallet address or unique transaction reference number for each transfer.

26.14.11 In processing virtual asset transfers, every licensed or authorised VASP shall screen the originator, beneficiary and wallet addresses and shall take freezing action and prohibit transactions with designated persons in accordance with Section 26.8.

26.14.12 Every licensed or authorised VASP shall use a Travel Rule solution that enables the secure and immediate transmission of required information, is interoperable with the solutions used by its counterparties, and uses a recognised data standard such as IVMS101, as may be further specified by the Bank by circular.

26.14.13 The processing of personal data under this section constitutes processing necessary for compliance with a legal obligation under the Nigeria Data Protection Act, 2023, and shall be subject to the data security, purpose limitation and confidentiality requirements of that Act.

26.14.14 A VASP shall conduct counterparty VASP due diligence in accordance with Section 26.16.

26.14.15 Every licensed or authorised VASP shall conduct periodic testing, monitoring and audit of its compliance with the requirements of this Section and shall promptly remediate and report to the Bank any material deficiencies identified in the implementation of the Travel Rule.

26.14.15 The Bank shall, as part of its risk-based supervision, conduct or require supervisory testing of a licensed or authorised VASP's Travel Rule systems, controls and procedures, and shall require the VASP to remediate any deficiencies identified within such period as the Bank may prescribe.

26.15 Transfers Involving Unhosted Wallets

26.15.1 Where a licensed or authorised VASP sends virtual assets to, or receives virtual assets from, an unhosted wallet, it shall obtain the required information in 26.14.3 or 26.14.4 from its customer and retain it in accordance with Section 26.12.

26.15.2 For transfers equal to or above the threshold in 26.14.3, the licensed or authorised VASP shall take reasonable measures to verify that its customer owns or controls the unhosted wallet, such as a message-signing or micro-transfer test.

26.15.3 The licensed or authorised VASP shall assess and mitigate the AML/CFT/CPF risks of unhosted-wallet transfers on a risk-sensitive basis. Depending on the risks, measures may include blockchain analytics screening of the wallet and its transaction history, enhanced due diligence, transaction limits, and refusing or suspending the transfer.

26.16 Counterparty VASP Relationships

26.16.1 Before establishing a relationship with, or transferring virtual assets to or from, another VASP, and on an ongoing basis, a licensed or authorised VASP shall conduct counterparty due diligence to:

a) gather sufficient information about the counterparty to understand fully the nature of its business, including its ownership, beneficial ownership, management, place of incorporation and operation, and to determine from publicly available information its reputation, regulatory history and whether it has been subject to any AML/CFT/CPF or sanctions investigation or regulatory action;

b) confirm that the counterparty is licensed or registered and supervised for AML/CFT/CPF purposes in the jurisdiction(s) where it operates;

c) assess the counterparty's AML/CFT/CPF and sanctions controls; and

d) confirm that the counterparty can comply with Travel Rule requirements and protect the confidentiality of the information transmitted.

26.16.2 A licensed or authorised VASP shall obtain senior management approval before establishing a new counterparty relationship involving custody, liquidity, settlement, nested services or direct customer access, and before continuing any higher-risk counterparty relationship.

26.16.3 A licensed or authorised VASP shall clearly understand and document the respective AML/CFT/CPF responsibilities of each party. Where a counterparty's customers have direct or indirect access to the licensed or authorised VASP's services, the licensed or authorised VASP shall be satisfied that the counterparty has conducted CDD on those customers and can provide relevant CDD information upon request.

26.16.4 Where a counterparty relationship involves nested services, or otherwise enables another VASP or the customers of another VASP to access the licensed or authorised VASP's services directly or indirectly, the licensed or authorised VASP shall apply enhanced counterparty due diligence proportionate to the risks. Such due diligence shall include identifying any underlying VASP and its beneficial owners; assessing its licensing or registration status, jurisdiction of operation and AML/CFT/CPF controls;

understanding the nature and risk profile of its customer base and transaction activities; ensuring that relevant underlying customer information can be obtained promptly upon request; monitoring indirect and third-party exposures arising through the relationship; and periodically reassessing the relationship. The licensed or authorised VASP shall restrict, suspend or terminate the nested relationship where the risks cannot be adequately mitigated or the required information cannot be obtained.

26.16.5 A licensed or authorised VASP shall not enter into or continue a relationship with a shell bank, a shell VASP, or an unlicensed or unregistered VASP, and shall satisfy itself that its counterparties do not permit their services to be used by such entities.

26.16.6 A licensed or authorised VASP shall treat as higher-risk, and apply enhanced counterparty due diligence to, a VASP incorporated or operating in a jurisdiction that does not effectively license or register VASPs, or whose licensing or supervisory status cannot be verified.

26.16.7 A licensed or authorised VASP shall treat as higher-risk, and apply enhanced counterparty due diligence to, a VASP incorporated or operating in a jurisdiction that does not effectively license or register VASPs, or whose licensing or supervisory status cannot be verified.

26.16.8 A Licensed Issuer or licensed or authorised VASP shall not provide services, including Naira on-ramp or off-ramp, settlement, liquidity or account services, to or for the benefit of a person named on the list under Section 52.6, and shall report to the Bank, and where appropriate to the NFIU, any attempt by that person, or by a person it reasonably suspects to be carrying on a Regulated Activity without authorisation, to obtain such services.

26.17 Due Diligence at Issuance and Redemption

26.17.1 A Licensed Issuer shall issue (mint) stablecoins only to customers on whom CDD has been completed in accordance with Section 26.3.

26.17.2 A Licensed Issuer shall redeem stablecoins only for a customer on whom CDD has been completed and remains current in accordance with its risk-based review cycle under Section 26.3.8. It shall update CDD before redemption where a trigger event, unusual activity or a material change in the customer's risk profile has been identified.

26.17.3 Where a holder who is not a customer of the Licensed Issuer seeks to redeem directly, the issuer shall complete CDD on that holder before processing the redemption.

26.17.4 Redemption proceeds shall be paid only to an account held in the name of the verified customer at a bank or other financial institution licensed by the Bank or, for a foreign customer, at a financial institution subject to equivalent AML/CFT/CPF supervision.

26.18 Freeze, Block and Reissue Capability

26.18.1 A Licensed Issuer shall issue (mint) stablecoins only to customers on whom CDD has been completed in accordance with Section 26.3.

26.18.2 A Licensed Issuer shall maintain the technical capability, policies and procedures to freeze, block and reject transfers of its stablecoin and, where lawfully ordered, to burn and reissue it, in both primary and secondary markets.

26.18.3 A Licensed Issuer shall secure the administrative keys or functions that control freezing, blocking, burning and reissuance through multi-party authorisation and segregation of duties, and shall keep a log of every use of those functions.

26.18.4 A Licensed Issuer shall report every use of the functions in 26.18.1 to the Bank, and to the NFIU where the action relates to suspected AML/TF/PF or sanctions, within twenty-four (24) hours.

26.19 Secondary-Market Monitoring and Deny-Listing

26.19.1 A Licensed Issuer shall monitor, using blockchain analytics, wallets holding or transacting in its stablecoin, whether or not the holder is its customer, to identify wallets associated with designated persons, sanctions evasion, fraud, ransomware, terrorist financing or other unlawful activity.

26.19.2 A Licensed Issuer shall maintain a deny-list of wallets identified under 26.19.1 and shall freeze or block the stablecoins held by such wallets where required by Section 26.8, a lawful order, or its risk-based policies approved by the board.

26.19.3 A Licensed Issuer shall file a suspicious transaction report under Section 26.9 in respect of suspicious secondary-market activity in its stablecoin, whether or not the persons involved are its customers.

26.19.4 A Licensed Issuer shall share its deny-list with the Bank and the NFIU upon request, and with licensed or authorised VASPs distributing its stablecoin to the extent permitted by law.

26.20 Networks, Bridges and Smart Contracts

26.20.1 A Licensed Issuer shall issue its stablecoin only on blockchain networks on which it can exercise the controls in Section 26.18.

26.20.2 A Licensed Issuer shall complete the risk assessment in 26.1.4 before deploying its stablecoin on any new network or bridge, or changing any smart-contract function, and shall notify the Bank at least thirty (30) days in advance.

26.20.3 A Licensed Issuer shall ensure that its smart contracts are independently audited before deployment and after any material change, including for the effectiveness of the freeze, block, burn and reissue functions.

26.20.4 Where its stablecoin is bridged or wrapped on a network where it cannot exercise the controls in Section 26.18, the Licensed Issuer shall assess the resulting AML/TF/PF risks, apply mitigating measures, and inform the Bank.

26.21 Distributors and Intermediaries

26.21.1 Before appointing a VASP, financial institution or other person to distribute, offer, exchange or custody its stablecoin, a Licensed Issuer shall conduct due diligence equivalent to that in 26.16.1, and shall obtain senior management approval.

26.21.2 A Licensed Issuer shall enter into a written agreement with each distributor that allocates AML/CFT/CPF responsibilities, including CDD, Travel Rule compliance, sanctions screening, suspicious transaction reporting and the provision of customer and transaction information to the issuer upon request without delay.

26.21.3 A Licensed Issuer shall not appoint, and shall terminate, a distributor that is unlicensed or unregistered where licensing or registration is required, or that fails to maintain adequate AML/CFT/CPF controls.

26.21.4 The appointment of a distributor shall not relieve the Licensed Issuer of its obligations under this Part.

26.22 Application of transfer and counterparty requirements to issuers

26.22.1 Where a Licensed Issuer transfers its stablecoin to or from a wallet on issuance, on redemption or otherwise on behalf of a customer, Section 26.14 and Section 26.15 shall apply to it as if it were a licensed or authorised VASP.

26.22.2 Where a Licensed Issuer transfers its stablecoin to or from another VASP, or has a business relationship with another VASP other than as a distributor under Section 26.21, Section 26.16 shall apply to it as if it were a licensed or authorised VASP.

26.23 Decentralised arrangements: A person that has control of, or sufficient influence over, an arrangement that provides a service in Section 9.1, including through governance rights, administrative keys, a front-end interface or the ongoing receipt of fees, shall be treated as providing that service. Describing an arrangement as decentralised, or the use of smart contracts, shall not of itself remove the arrangement from the scope of these Regulations.

Part 8
Customer Protection and Conduct

Section 27 Obligations Towards Customers and Complaints

Disclosures and Business Conduct

27.1 Every Licensed Issuer shall publish and maintain on its publicly accessible website the following information at all times:

a) the current Stablecoin Whitepaper as prescribed in Schedule 5;

b) the current terms and conditions governing the issuance, holding, and redemption of the stablecoin;

c) the fee schedule applicable to minting, redemption, and other transactions;

d) the names and registered addresses of all reserve asset custodians;

e) the most recent reserve attestation report;

f) any regulatory notices, directives, or conditions issued by the Bank in respect of the stablecoin; and

e) contact information for the issuer's complaints management function.

27.2 The display notice specified in 8.7.2 shall clearly indicate that the Bank does not guarantee the token or its obligations.

27.3 Every Licensed Issuer shall disclose material changes to the information specified in Section 27.1 within forty-eight (48) hours of such change. Material changes include but are not limited to changes in reserve asset composition, changes in custodians, changes in the underlying blockchain networks, and changes in governance arrangements.

27.4 Advertising, marketing, and promotional materials relating to any Regulated Token shall:

a) be fair, clear, and not misleading;

b) clearly state, except in the case of a Deposit Money Token, that the token is not a bank deposit and is not covered by the Nigeria Deposit Insurance Corporation (NDIC) guarantee scheme:

c) clearly state, except in the case of a Deposit Money Token, that holding the token does not entitle the holder to interest or yield; and

c) include a risk warning in terms approved by the Bank.

Complaints Management

27.5 Every Licensed Issuer shall establish, maintain, and publish a written complaints management policy covering:

a) the process by which holders may submit complaints, including the contact details of the dedicated complaints management function;

b) the maximum time within which the issuer shall acknowledge receipt of a complaint, which shall not exceed two (2) Business Days;

c) the maximum time within which the issuer shall provide a final response to a complaint, which shall not exceed twenty (20) Business Days, or such longer period as may be agreed with the complainant in writing;

d) escalation procedures for complaints that cannot be resolved at the first level; and

e) the process for referring unresolved complaints to the Bank's consumer protection function.

27.6 The Licensed Issuer shall maintain a register of all complaints received, the nature of each complaint, and the outcome and resolution timeline. The complaints register shall be submitted to the Bank as part of the quarterly regulatory report prescribed in Schedule 7.

27.7 Service providers shall give customers clear and accurate information appropriate to their approved services and maintain effective channels for enquiries, error reports, fraud reports and complaints. Issuer-specific disclosures, redemption protections and the no-yield rule shall not be diluted by use of an intermediary.

Section 28 Stablecoin Whitepapers

28.1 **Obligation to publish:** Every Licensed Issuer shall prepare, obtain the Bank's approval for and publish a Whitepaper before issuance. The Whitepaper shall remain freely accessible on its website and identify the Licensed Issuer, the Regulated Token and material service arrangements.

28.2 **Content and Form:** The Whitepaper shall contain the information in Schedule 5, be accurate, complete in material respects, clear and consistent with customer terms, and explain the reference asset, backing, redemption, governance, technology, risks, regulatory status and absence of a CBN guarantee.

28.3 **Updates:** The issuer shall keep the Whitepaper current, obtain approval for material changes where required and disclose material changes within forty-eight hours in accordance with Section 27. A change to the Whitepaper shall not itself authorise a change to the licence, reserve rules or customer rights.

28.4 **Audit and Verification:** The Whitepaper's reserve and technical statements shall be supported by the applicable independent reserve attestations, smart contract audits and legal opinions. The Bank may require verification or correction. A Whitepaper shall not substitute for any assurance required by Sections 7, 24 or 37.

28.5 **Notification and Responsibility:** The issuer shall submit the Whitepaper and proposed material revisions to the Bank through the designated channel. The issuer remains responsible for its contents and shall promptly correct material inaccuracies and notify affected holders. Liability for misleading statements shall be determined under applicable law and Section 51.

28.6 **Exemptions:** No issuer shall omit a mandatory disclosure unless the Bank has expressly permitted that omission under a lawful exemption specifying its scope and conditions. No exemption shall remove a holder's statutory rights or disguise an unapproved token.

Section 29 Customer Agreements

29.1 Before providing a regulated service, the provider shall make its Customer Agreement available in a durable and accessible form, identify the contracting entity and approved service and obtain the customer's acceptance. It shall retain evidence of the agreement and subsequent changes.

29.2 The agreement shall be clear, fair and consistent with these Regulations. It shall not waive mandatory redemption, asset-safeguarding, privacy, complaints or other protections. Material changes shall be communicated before implementation where practicable and remain subject to any required approval and customer rights under applicable law.

Section 30 Required Terms and Pre Contractual Information

30.1 Before contracting, the provider shall disclose its identity, contact details, licence or authorisation, service scope, token and issuer, custody and safeguarding arrangements, customer eligibility and verification requirements, and the nature of the customer's legal claim.

30.2 Terms shall explain issuance and redemption where relevant; charges and conversion-rate methodology; authorisation and execution of transfers; settlement and finality; technical and operational risks; suspension, freezing and lawful blocking; error and unauthorised-transaction procedures; complaints and escalation; termination; and the return or transfer of assets.

30.3 Stablecoin terms shall state the par-redemption right, one-business-day processing requirement, no standard redemption fee, permitted suspension grounds, reserve protection, no-yield rule and absence of deposit insurance. DMT terms shall describe the deposit claim and actual insurance treatment under Section 40. Disclosures shall not imply a product has protections applicable only to another token category.

Section 31 Transactional Information

31.1 The provider shall make available an identifiable record of each customer transaction, including transaction reference, date and time, token, amount, applicable charges, conversion rate and fiat amount where relevant, destination or counterparty information lawfully disclosable, and execution or settlement status.

31.2 Information shall distinguish a submitted, pending, completed, failed, rejected, frozen or reversed transaction and identify available error or dispute channels. Customer balances and statements shall reconcile to the provider's underlying records. Mandatory AML/CFT confidentiality and data-protection restrictions shall apply.

Section 32 Protection of Payment and Personal Data

32.1 Every regulated entity shall comply with the Nigeria Data Protection Act 2023 and applicable security, confidentiality and lawful-disclosure requirements. It shall maintain policies and controls against unauthorised access, alteration, misuse, loss and disclosure of customer, payment, wallet and identity data.

32.2 Processing, retention, sharing and cross-border access shall have a lawful basis and be limited to legitimate purposes. Outsourcing shall preserve appropriate safeguards and lawful access by the Bank, NFIU and other competent authorities. Travel Rule data shall be transmitted securely and kept available under Section 26.

32.2 The entity shall maintain access restrictions, secure backups, incident response and records sufficient to demonstrate compliance. Data incidents shall be reported under Section 20 and any separate applicable legal notification duty. No requirement to disclose information shall authorise tipping off or public disclosure of confidential suspicious transaction reports.

Section 33 Unauthorised Transfers Errors Liability and Refunds

33.1 A provider shall maintain accessible procedures for customers to report suspected unauthorized transfers, errors, fraud or loss of credentials and shall promptly secure affected accounts or assets, preserve evidence, investigate and inform the customer of the outcome, subject to lawful restrictions on disclosure.

33.2 Where a loss or unauthorised transfer is attributable to the provider's breach of its obligations, it shall make the refund, restoration or compensation due under applicable law and the Customer Agreement. Liability shall not be excluded by a term inconsistent with mandatory law or these Regulations. The provider shall maintain evidence of transaction authorisation, authentication, execution and relevant controls.

33.3 The customer shall be informed of the investigation and any amount and basis of redress. Disputes shall follow Section 27, including the prescribed complaints response deadlines and escalation to the Bank. The Bank may prescribe further refund procedures and timelines.

Section 34 Certainty and Finality of Transfers

34.1 The provider shall assess the resilience and settlement characteristics of each supported network and document when a transfer is accepted, executed and treated as final. The Whitepaper and Customer Agreement shall explain confirmation requirements, material risks of congestion, forks, reversal and network failure, and applicable procedures for failed or disputed transfers.

34.2 The provider shall maintain a complete audit trail and arrangements for reconciliation, error handling, lawful freezing and dispute resolution. A technical failure shall not extinguish an established holder entitlement or relieve the issuer of redemption obligations. Competing claims shall be resolved through verified records and applicable law without duplicate payment.

34.3 Interbank DMT transfers shall follow Section 43, including approved settlement infrastructure and conversion at par. No disclosure about blockchain timing shall override a prescribed redemption deadline or an enforceable customer protection.

Part 9
Governance Risk and Technology

Section 35 Corporate Governance

35.1 Issuers shall comply with applicable CBN governance directives. An issuer's board shall have at least five members, including at least two independent non-executive directors and at least one member with demonstrable financial services, banking or fintech regulatory expertise. Its audit committee shall comprise at least three members, a majority independent non-executive directors; its risk committee shall comprise at least three members. It shall have a Chief Executive Officer, Chief Compliance Officer and Chief Risk Officer approved by the Bank, board-approved policies and an internal audit function independent of management.

35.2 Boards shall approve policies for reserves, redemption, AML/CFT/CPF, technology security, outsourcing, business continuity and complaints and oversee their effectiveness. Audit committees shall oversee financial reporting, reserves and the independent auditor; risk committees shall oversee reserve, operational, technology and liquidity risks. Internal audit shall be independent of management.

35.3 Other-service providers shall maintain governance appropriate to their principal licensing framework, approved activities and risk profile, together with additional conditions imposed by the Bank. Appointment, approval and replacement of directors, controllers and senior management shall be governed by Section 18.

Section 36 General Risk Management and Internal Control Systems

Risk Management Framework

36.1 Every Licensed Issuer shall maintain a comprehensive, board-approved risk management framework addressing:

a) **Reserve Risk:** the risk that the value of reserve assets falls below the value of stablecoins in circulation, including interest rate risk, credit risk, and currency risk in respect of reserve assets;

b) **Liquidity Risk:** the risk that the issuer is unable to meet redemption obligations in a timely manner, including scenarios of concentrated redemption demand;

c) **Operational Risk:** the risk of loss from inadequate or failed internal processes, people, or systems, or from external events, including the risk of smart contract failures, key management failures, and platform outages;

d) **Technology and Cybersecurity Risk:** the risk of loss from cyberattacks, data breaches, and unauthorised access to reserve accounts or smart contract control keys, and the risk of vulnerabilities in the issuer's blockchain infrastructure;

e) **Compliance Risk:** the risk of legal or regulatory sanction arising from failure to comply with these Regulations and applicable laws; and

f) **Concentration Risk:** the risk arising from over-reliance on a single reserve custodian, blockchain network, technology vendor, or distribution partner.

36.2 The risk management framework shall be reviewed and approved by the board annually and whenever material changes occur in the issuer's operations or risk profile.

Capital Adequacy and Capital Planning

36.3 The entity shall monitor and plan for continuing capital compliance under Sections 15–17, including losses, growth, concentration and stressed conditions. A capital deposit shall not be treated as unencumbered operational liquidity.

Liquidity Risk Management

36.4 Issuers shall maintain the liquid assets in Section 17 and the reserve liquidity, maturity, reconciliation and stress arrangements in Section 24. Other providers shall maintain resources appropriate to customer withdrawals, settlement and operational continuity.

36.5 A Licensed Issuer shall establish and maintain a documented Reserve Asset Risk Management Framework designed to identify, measure, monitor and control risks arising from the management of the Reserve Pool. The Framework shall include:

a) a liquidity management policy covering the maintenance of adequate liquidity to satisfy redemption requests;

b) procedures for monitoring liquidity mismatches and concentration risks;

c) policies governing the use of repos, reverse repos and other liquidity management transactions;

d) periodic liquidity stress testing under normal and stressed market conditions; and

e) a liquidity contingency funding plan addressing significant redemption events, market disruptions and Reserve Pool shortfalls.

The issuer shall maintain records demonstrating compliance with this Section and shall make such records available to the Bank upon request.

Internal Controls

36.6 The entity shall maintain documented responsibilities, segregation of duties, approvals, reconciliations, access controls and escalation of exceptions proportionate to its activities. It shall monitor conflicts, fraud, outsourcing and dependencies on custodians, banks, networks and technology providers.

36.7 Accounting and External Audit

36.7.1 The entity shall maintain accurate financial and token records, separate its own assets from customer assets and reserves and reconcile the relevant records.

Issuer annual financial audits and reserve attestations shall comply with Sections 20 and 24. Other providers shall submit audited financial information as required by their licence and principal regulatory framework.

36.8 Compliance and Internal Audit Functions

36.8.1 Compliance shall have sufficient authority, resources and access to information and the board. Independent audit shall test controls and track remediation. The detailed AML/CFT/CPF compliance and audit requirements in Section 26 shall apply.

36.9 Reputation Risk Management

36.9.1 The entity shall monitor complaints, misleading promotion, conflicts, service failures and other events affecting public confidence and promptly address their causes. Disclosures shall accurately reflect the entity's approvals and operational capacity.

36.10 Record Keeping

36.10.1 Records shall be complete, secure, retrievable and reconcilable to on-chain, banking, custody and customer systems. Section 26 retention minima and preservation duties shall apply to AML/CFT/CPF records; other records shall be retained for the applicable legal or prescribed period. No destruction shall frustrate an investigation, order or supervisory request.

Section 37 Technology Risk and Information Security

Cybersecurity and Smart Contract Controls

37.1 Every Licensed Issuer and licensed or authorised VASP shall implement and maintain a comprehensive cybersecurity framework that meets or exceeds the standards prescribed in the CBN Cybersecurity Framework for Banks and Other Financial Institutions, as applicable to Licensed Issuers, and shall address:

a) the security of smart contract private keys and administrative credentials, including the use of hardware security modules (HSMs), multi-signature key management, and geographic distribution of key custodians;

b) the security of reserve account access credentials and custodian interfaces;

c) network security, including firewalls, intrusion detection systems, and network segmentation;

d) employee access controls, including role-based access and privileged access management;

e) incident detection and response capabilities, including 24/7 monitoring of smart contract and platform activity; and

f) protection of customer data in compliance with the Nigeria Data Protection Act, 2023.

37.2 Every Licensed Issuer and licensed or authorised VASP shall conduct an annual penetration test of its technology infrastructure, conducted by an independent cybersecurity firm approved by the Bank, and submit the results of such test to the Bank within thirty (30) days of completion.

37.3 Every Licensed Issuer shall ensure that the smart contracts governing its stablecoin incorporate the following mandatory technical controls:

a) **Freeze capability:** the ability to freeze a specific wallet address or token balance pursuant to a lawful court order, regulatory directive, or NFIU instruction, preventing further transfers from or to the frozen address;

b) **Burn capability:** the ability to permanently retire (burn) stablecoin tokens held in a frozen or confiscated address, pursuant to a lawful court order or regulatory directive;

c) **Deny-listing:** the ability to block transactions to or from wallet addresses identified by the Bank, the NFIU, or competent law enforcement authorities as being associated with money laundering, terrorist financing, proliferation financing, or sanctions violations;

d) **Allow-listing (optional, for institutional-only deployment):** the ability to restrict transfers to pre-approved wallet addresses where the issuer's operational model requires a closed participant set;

e) **Upgrade capability:** the ability to upgrade or patch the smart contract logic to address security vulnerabilities or regulatory changes, subject to multi-signature governance controls and advance notification to the Bank; and

f) **Pause capability:** the ability to temporarily suspend all token transfers in the event of a material security incident, subject to immediate notification to the Bank.

37.4 Exercise of freeze, burn or deny-listing powers shall be governed by documented procedures approved by the Board and shall be subject to audit trails, access controls and legal authorization requirements.

37.5 Prior to launching or materially upgrading its stablecoin platform, every Licensed Issuer shall obtain a smart contract audit from at least two (2) independent, reputable smart contract security firms and shall submit the audit reports to the Bank. The Bank may refuse to permit the launch or upgrade where audit findings reveal material security vulnerabilities that have not been remediated.

37.6 Operational Resilience

37.6.1 Every Licensed Issuer shall design its operational architecture to ensure that its stablecoin platform can withstand operational disruptions, including blockchain network congestion, smart contract failures, and custodian system outages, and shall define and publish target operational resilience standards, including:

a) a maximum acceptable downtime for the issuance and redemption platform, which shall not exceed four (4) hours per calendar quarter;

b) recovery time objectives (RTOs) and recovery point objectives (RPOs) for all critical systems; and

c) a multi-network deployment strategy for Class 1 Stablecoins issued on public blockchain networks, to ensure that disruption of a single blockchain network does not prevent all issuance and redemption activity.

37.7 IT Governance

37.7.1 The board shall oversee technology risks, approve security policies and ensure qualified responsibility for architecture, access, change management and material smart contract upgrades. Critical systems and providers shall be identified and monitored.

37.8 Security Requirements

37.8.1 The entity shall secure private keys, administrative credentials, customer access and reserve interfaces using appropriate cryptography, controlled privileges, segregation of duties and audit trails. Controls shall support lawful freezing, blocking and other approved functions without unauthorised use.

37.9 Network and Infrastructure Management

37.9.1 The entity shall maintain resilient infrastructure, controlled configuration and patching, capacity monitoring, backups and recovery arrangements. Material network, bridge and contract changes shall undergo risk assessment, independent testing and the notification or approval required by these Regulations.

37.10 Cybersecurity Risk

37.10.1 Threat monitoring, vulnerability management and response shall operate on a continuing basis. Independent testing and smart contract audits shall meet the requirements in this Section, including annual penetration testing and submission within thirty days and at least two independent smart contract security audits before launch or material upgrade.

Customer Authentication

37.11 Authentication and access controls shall be proportionate to transaction and account risks and protect against credential theft and unauthorised transfers. Sensitive changes and transaction authorisation shall be verifiable and recorded.

Login Attempts and Session Management

37.12 The provider shall detect repeated failed logins and anomalous sessions, apply controls against automated attacks and account takeover and protect session credentials. It shall maintain risk-based session termination and re-authentication controls.

Fraud Detection Systems

37.13 The provider shall monitor suspicious device, access, wallet and transaction patterns and promptly investigate fraud alerts. Fraud controls shall work alongside the AML/CFT/CPF monitoring and sanctions systems required by Section 26.

Security Advice for Customers

37.14 The provider shall give clear advice on protecting credentials, verifying transaction details, recognising scams and promptly reporting suspected compromise. Customer advice shall not replace the provider's own security and asset-protection duties.

Security Incident Reporting

37.15 Cybersecurity and other technology incidents shall be notified under Section 20. The entity shall preserve evidence, contain harm, restore service, provide the prescribed follow-up report and complete remediation and prevention measures.

Section 38 Business Continuity Recovery and Orderly Wind Down

Business Continuity Planning

38.1 Every Licensed Issuer shall maintain a Board-approved Business Continuity Plan (BCP) addressing:

a) procedures for maintaining issuance and redemption services during operational disruptions;

b) procedures for transitioning platform operations to backup infrastructure in the event of primary infrastructure failure;

c) communication protocols for notifying the Bank, holders, and distribution partners in the event of a material operational incident;

d) arrangements with alternative blockchain networks or off-chain settlement mechanisms as a contingency for blockchain network failure; and

e) procedures for the orderly wind-down of operations if required.

Cessation and Winding Up

38.2 Where a Licensed Issuer becomes insolvent, enters liquidation, administration, receivership or winding-up, or is otherwise unable to meet its obligations as they fall due, it shall notify the Bank immediately and comply with all applicable statutory and regulatory requirements.

38.3 A Licensed Issuer shall not voluntarily cease or materially discontinue its stablecoin issuance or redemption operations without prior written notification to the Bank. Where the Bank suspends or revokes a licence or directs the cessation of activities, the issuer shall comply with the Bank's directions.

38.4 Every Licensed Issuer shall maintain a Board-approved wind-down plan, subject to the Bank's requirements, setting out the arrangements for:

a) cessation of new stablecoin issuance;

b) notification to stablecoin holders, distribution partners, custodians and other relevant counterparties;

c) continued redemption of outstanding stablecoins, subject to applicable law and any directions of the Bank;

d) preservation, reconciliation, segregation and orderly administration of reserve assets;

e) preservation of records and submission of final regulatory reports; and

f) the orderly termination or transfer of critical operational functions.

38.5 The issuer shall maintain appropriate arrangements for the redemption of outstanding stablecoins and shall not apply reserve assets attributable to such stablecoins to general corporate expenses.

38.6 Upon cessation of operations, the Licensed Issuer shall safeguard the reserve assets corresponding to outstanding stablecoins and maintain records of unredeemed claims. The Bank may direct the transfer of unclaimed redemption proceeds, following conversion into the relevant fiat currency where necessary, to a designated or approved arrangement for the benefit of eligible holders, subject to applicable law.

38.7 The Bank may require an issuer to revise or implement its wind-down plan, provide additional information, appoint an independent person to oversee the cessation process, or take other measures within the Bank's lawful powers to protect holders and preserve the orderly administration of outstanding obligations.

38.8 Where cessation occurs in connection with insolvency, liquidation, administration, receivership or winding-up, this Section shall operate subject to applicable insolvency legislation and the powers of the relevant court, liquidator, receiver, administrator or other duly appointed office-holder.

38.9 Other-service providers shall maintain continuity and wind-down arrangements appropriate to their services, including return or approved transfer of customer assets. Agency and outsourcing arrangements shall support continuity. Surrender, suspension and revocation shall be governed by Section 14 and shall not discharge outstanding obligations.

Part 10
Deposit Money Tokens

Section 39 Definition of Deposit Money Tokens

39.1 For the purposes of these Regulations, a Deposit Money Token (DMT) means a digital token issued by a CBN-licensed bank which represents a direct claim on that bank and corresponds to an existing deposit liability denominated in Naira.

Section 40 Legal Status and Deposit Treatment

40.1 A DMT shall constitute a representation of an existing deposit liability of the Issuing Bank and shall not constitute a separate form of money or a new category of deposit-taking instrument.

40.2 A DMT shall rank as a deposit claim against its Issuing Bank under applicable banking and insolvency law. Deposit insurance shall be determined under applicable law and arrangements with the NDIC; the stablecoin exclusion from deposit insurance shall not determine DMT treatment.

Section 41 Eligibility and Approval to Issue Deposit Money Tokens

41.1 Only a Deposit Money Bank licensed by the CBN may issue DMTs under these Regulations.

41.2 A bank intending to issue DMTs shall obtain the prior written approval of the CBN.

41.3 The CBN may, as a condition of approval, require an applicant to demonstrate:

a) adequate technological and operational capacity;

b) appropriate risk management arrangements;

c) adequate systems for reconciliation of DMTs with underlying deposit liabilities;

d) arrangements for customer protection and dispute resolution; and

e) compliance with any additional requirements specified by the CBN.

Section 42 Issuance Backing and Redemption

42.1 Every DMT issued by a bank shall correspond to an equivalent deposit liability recorded in the books of the Issuing Bank.

42.2 The Issuing Bank shall maintain continuous reconciliation between:

a) the outstanding quantity/value of DMTs in circulation; and

b) the corresponding deposit liabilities recorded in its core banking or designated deposit ledger.

42.3 A DMT holder shall be entitled to redeem the DMT at par value against the underlying deposit, subject to applicable law and the terms prescribed by the CBN.

42.4 The Issuing Bank shall establish and maintain procedures for the prompt redemption and settlement of DMTs.

42.5 A DMT shall rank as a deposit claim against the Issuing Bank in accordance with applicable banking and insolvency laws.

42.6 The treatment of DMTs for purposes of deposit insurance shall be determined in accordance with applicable law and arrangements agreed with the Nigeria Deposit Insurance Corporation.

Section 43 Transfer and Settlement

43.1 A DMT may be transferred between customers of the Issuing Bank in accordance with the conditions approved by the CBN.

43.2 Interbank transfer of DMTs shall be effected only through a settlement mechanism approved or designated by the CBN.

43.3 The CBN may require interbank DMT transactions to settle through the Real-Time Gross Settlement System or another CBN-approved settlement infrastructure.

43.4 Where DMTs issued by different banks are exchanged, the settlement mechanism shall provide for conversion at par and shall prevent the creation of separate or fragmented forms of Naira commercial-bank money.

43.5 The CBN may prescribe standards for the interoperability of DMT platforms, including standards relating to:

a) Settlement;

b) Tokenisation;

c) messaging and transfer;

d) identification; and

e) technical connectivity.

43.6 Interbank transfers of DMTs shall settle in central bank money through the Bank's RTGS system or such other settlement arrangement as the Bank may approve, and settlement shall be final and irrevocable once effected in that system. An Issuing Bank shall ensure that its DMTs are interoperable with the DMTs of other Issuing Banks in accordance with the standards prescribed under Section 43.5.

Section 44 Wallets Custody and Third Party Participation

44.1 An Issuing Bank shall be responsible for the custody and administration of DMTs issued by it, unless otherwise approved by the CBN.

44.2 A bank may use a third-party technology or payment service provider in connection with DMT activities, subject to applicable CBN requirements.

44.3 A third party providing services that enable the holding, transfer, settlement or administration of DMTs shall comply with such licensing, registration, operational and risk-management requirements as may be prescribed by the CBN.

44.4 The use of a third-party service provider shall not relieve the Issuing Bank of its regulatory obligations under these Regulations.

Section 45 Permitted Uses and Programmability

45.1 DMTs may be used for such payment, settlement and other financial activities as may be approved by the CBN.

45.2 The CBN may designate certain DMT use cases as:

a) generally permitted;

b) subject to prior approval; or

c) prohibited or deferred.

45.3 A bank shall not deploy a programmable or smart-contract-based DMT arrangement that may materially affect a customer's funds without appropriate controls for:

a) authorisation;

b) error correction;

c) dispute resolution; and

d) where appropriate, human intervention or override.

45.4 DMTs used for securities settlement, tokenised assets, digital-asset transactions or other activities falling within the regulatory mandate of another competent authority shall comply with the requirements applicable to that activity.

Section 46 Risk Management AML and Customer Protection

46.1 Risk Management

A bank issuing DMTs shall identify, assess, monitor and manage risks arising from its DMT activities in accordance with applicable CBN risk-management requirements.

The bank shall maintain appropriate controls for technology, operational, liquidity, settlement, fraud and cybersecurity risks associated with DMTs.

46.2 All DMT activities shall comply with applicable AML/CFT laws, regulations and CBN requirements. The Issuing Bank shall ensure that appropriate customer due diligence and sanctions screening are undertaken before permitting transfers involving persons or entities that are not appropriately identified or verified.

46.3 Consumer Protection

A bank issuing DMTs shall provide customers with clear information on:

a) the nature of the DMT;

b) the underlying deposit claim;

c) redemption arrangements;

d) applicable fees;

e) applicable deposit-insurance treatment; and

f) applicable risks and limitations.

46.4 A bank shall maintain procedures for handling customer complaints, erroneous transfers, fraud and disputes involving DMT transactions.

Section 47 Reporting and Supervisory Requirements

47.1 A bank issuing DMTs shall maintain complete and accurate records of:

a) DMT issuance;

b) Outstanding DMTs;

c) Redemption;

d) Transfers;

e) Settlement; and

f) Other information prescribed by the CBN.

47.2 The CBN may require an Issuing Bank to provide real-time or near-real-time access to DMT transaction and settlement information for supervisory purposes.

47.3 The Issuing Bank shall provide periodic reports to the CBN in such form and manner as may be prescribed.

Section 48 Cross Border Transactions

48.1 Cross-border DMT transactions shall comply with all applicable foreign exchange, capital-flow, AML/CFT and other regulatory requirements.

48.2 No DMT arrangement shall be used to circumvent applicable foreign exchange or capital-control requirements.

48.3 The CBN may prescribe additional requirements for cross-border DMT transactions, including transaction screening and reporting.

Section 49 Regulatory Pilot Arrangements

49.1 The CBN may authorise the testing of DMT products, platforms, settlement arrangements or use cases under its regulatory pilot or other controlled testing arrangements.

49.2 A pilot authorisation may be subject to limitations relating to:

a) duration;

b) participating institutions;

c) transaction volume;

d) customer numbers;

e) permitted use cases; and

f) other conditions determined by the CBN.

49.3 The CBN may suspend or withdraw a pilot authorisation where it considers that the activity presents material risks to customers, the institution or the financial system.

Section 50 DMT Supervision and Enforcement

50.1 The CBN shall supervise DMT activities undertaken by institutions under its regulatory purview.

50.2 The CBN may require an institution to modify, suspend or discontinue any DMT activity where the activity is inconsistent with these Regulations or presents material risk to the institution, its customers or the financial system.

50.3 A contravention of these Regulations shall attract such supervisory or regulatory action as may be prescribed by the CBN and applicable law.

Part 11 Enforcement and Administrative Sanctions

Section 51 Definition of Deposit Money Tokens

51.1 **Administrative Monetary Penalties:** In exercise of its powers under BOFIA (2020), CBN Act (2007), MLPPA, and TPPA, the Bank may impose the following administrative and monetary penalties on any person or entity including a person carrying on a Regulated Activity without the required licence, authorisation or approval, who fails to comply with these Regulations and, where permitted by applicable law and having regard to responsibility for the breach, on that person's directors, senior management, officers or key function holders:

a) for undertaking a Regulated Activity without the relevant licence, authorisation or Approval to Extend Permitted Activities required under these Regulations, or undertaking an activity outside the scope of such licence, authorisation or approval: a fine of not less than one hundred million naira (₦100,000,000) and an additional fine of not less than one million naira (₦1,000,000) for each day during which the contravention continues, without prejudice to any other penalty or enforcement action under BOFIA (2020) or other applicable laws;

b) for material breaches of BOFIA (2020) or liquidity requirements: a fine of not less than fifty million naira (₦50,000,000) and not more than two hundred and fifty million naira (₦250,000,000) per breach;

c) for breach of the prohibition on reserve leverage or encumbrance: a fine of not less than two hundred and fifty million naira (₦250,000,000) and not more than five hundred million naira (₦500,000,000) per breach;

d) for breach of AML/CFT/CPF obligations, including failure to file STRs, failure to apply CDD, or Travel Rule non-compliance: a fine of not less than fifty million naira (₦50,000,000) per breach, plus restitution of any amounts processed in violation of the obligation;

e) for breach of the prohibition on interest and yield payments to holders: a fine equivalent to twice the amount of the prohibited payment or benefit; and

f) for fraudulent or deliberate misrepresentation to the Bank or to the public in connection with reserve management or stablecoin operations: a fine of not less than five hundred million naira (₦500,000,000) and referral for criminal prosecution under applicable law.

51.2 Penalties shall be assessed having regard to the nature, gravity, and duration of the breach; the degree of culpability of the entity; the financial benefit obtained from the breach; the extent of harm caused to consumers or the financial system; and the entity's prior compliance record.

51.3 An entity against which a penalty is proposed shall be notified in writing and shall have fifteen (15) Business Days to make written representations to the Bank before the penalty is finalised. The Bank shall take representations into account in finalising the penalty.

51.4 Without prejudice to section 51.1, the Bank may take such enforcement or corrective measures as it considers appropriate in the circumstances including:

a) issuing a warning, caution or reprimand;

b) requiring the submission and implementation of a remedial action plan within such period as the Bank may specify;

c) directing the cessation, restriction or modification of any activity, product or service;

d) imposing additional prudential, operational, governance or reporting requirements;

e) restricting, suspending or withdrawing any licence, authorisation, approval or permission granted by the Bank;

f) imposing administrative monetary penalties in accordance with these Regulations and other applicable law;

g) requiring restitution or other remedial measures, where permissible and appropriate;

h) referring the matter to any competent regulatory or law enforcement authority; or

i) taking any other enforcement or supervisory action within the powers of the Bank under applicable law.

51.5 Enforcement shall operate with Sections 12 and 13. A direction affecting redemption shall comply with Section 23 and applicable lawful freezing or sanctions orders. Monetary penalties and any continuing-breach penalties shall have a lawful basis and remain subject to the notice, representation and proportionality requirements of these Regulations.

51.6 The Bank may publish administrative sanctions and refer suspected criminal conduct to competent authorities in accordance with applicable law. The exercise of supervisory powers shall not itself create statutory insolvency priority or immunity beyond that available under law.

Section 52 Eligibility and Approval to Issue Deposit Money Tokens

52.1 The Bank may conduct off-site and on-site supervision of any Licensed Issuer, Licensee, or other regulated entity within the scope of these Regulations. Supervisory activity may include examinations, inspections, independent reviews, meetings with directors and senior management, testing of systems and controls, review of reserves and redemption arrangements, and validation of regulatory returns.

52.2 The Bank may at any time issue a written request for information, documents, records, data, explanations, or access to systems relevant to its supervisory, monetary policy, financial-stability, foreign-exchange, consumer-protection, or enforcement functions. The recipient shall respond within the period specified by the Bank and shall ensure that records are complete, accurate, readily retrievable, and capable of reconciliation to the relevant ledger, blockchain, bank, custodian, or other source.

52.3 A refusal or failure to respond to an information request within the prescribed period shall constitute a compliance breach subject to the enforcement measures in Part 11.

52.4 The Bank may require information relevant to determining whether a person is carrying on an activity within scope, to the extent permitted by its enabling law and confidentiality requirements, and may enter information-sharing arrangements with the SEC, NFIU and other competent Nigerian or foreign authorities. An information-sharing arrangement shall not grant an otherwise unlicensed issuer or provider permission to operate.

52.5 For AML/CFT/CPF supervision, the Bank may conduct risk-sensitive inspections and reviews, require relevant records and direct remediation within a specified period, using its lawful powers. An outsourcing or group arrangement shall not prevent production of records. Any compulsory process shall remain subject to applicable statutory conditions.

52.6 **Unauthorised Regulated Activity:** Where the Bank has reasonable grounds to believe that a person is carrying on a Regulated Activity in or from Nigeria without the licence, authorisation or approval required under these Regulations or applicable law, or is otherwise unlawfully offering or providing such activity to persons in Nigeria, the Bank may, subject to applicable law:

52.6.1 The Bank shall maintain arrangements to identify persons carrying on a Regulated Activity without the licence, authorisation or approval required under these Regulations, including persons outside Nigeria whose activity is directed at persons in Nigeria. These arrangements shall draw on blockchain analytics, market and online monitoring, complaints, information from Licensees, financial institutions, the NFIU and other authorities, and suspicious transaction reports.

52.6.2 the Bank may, subject to applicable law:

a) issue a public warning or publish the name and relevant particulars of the person;

b) direct Licensees and financial institutions, within the scope of the Bank's regulatory authority, to take such lawful measures in relation to transactions involving that person as the Bank may specify;

c) notify or request the assistance of the Nigerian Communications Commission or any other competent authority in respect of access to, or use of, services connected with the unauthorised activity;

d) refer the matter to the NFIU, SEC, law-enforcement agencies or any other competent authority, as appropriate; and

e) take such other action as may be available to the Bank under applicable law.

52.6.3 Before listing under paragraph 52.6.2(a), the Bank shall, where practicable and where doing so would not prejudice the protection of consumers or the integrity of the financial system, notify the person and consider any representations within [five] Business Days. The Bank shall remove a person from the list where it is satisfied that the activity has ceased or has been authorised.

52.7 The Bank shall maintain and publish, in accordance with section 8.7.1, a register of all licences, authorisations and approvals granted under these Regulations, and a list of unauthorised persons identified under section 52.6.

52.8 International Cooperation: The Bank may, in accordance with the CBN Act, 2007; BOFIA, 2020 and other applicable law, exchange information on a Licensee, an applicant, or a person carrying on a Regulated Activity, with foreign competent authorities on virtual assets, VASPs and the matters governed by these Regulations, including AML, CTF and CPF.

52.8.1 A Licensee shall provide any information or assistance that the Bank requires in order to respond to a request from a foreign competent authority. A Licensee shall not rely on group, contractual or foreign secrecy obligations to withhold that information.

52.8.2 No cooperation arrangement between the Bank and a foreign authority shall grant any person permission to carry on a Regulated Activity in Nigeria.

52.8.3 Information exchanged shall be kept confidential and used only for its stated purpose. It shall not be disclosed further without the provider's prior consent, unless the law requires disclosure.

Section 53 Relationship with Other Regulatory Frameworks

53.1 These Regulations shall be read with applicable banking, payment-system, foreign-exchange, consumer-protection, data-protection and AML/CFT/CPF requirements. They shall not amend the SEC's statutory jurisdiction or automatically cancel an approval granted under another Nigerian framework.

53.2 The Bank shall coordinate overlapping licensing, supervisory, reporting and enforcement arrangements with competent authorities. An existing principal licence shall not dispense with the express CBN approval required for Non-Security Virtual Asset services. Any amendment to another CBN instrument shall be made expressly through the applicable process.

Section 54 Transition and Pilot Arrangements

54.1 Existing Operators: An existing operator shall apply for the appropriate licence or authorisation within one hundred and eighty calendar days of commencement of these Regulations. During that transition, it may continue only at its existing scale and subject to the Bank's interim conditions, provided it registers with the Bank within thirty days, complies with AML/CFT/CPF requirements from commencement, begins supervisory reporting within sixty days or an earlier prescribed period, and submits a complete application within the transition period. Failure to submit within that period shall require cessation until the required licence or authorisation is obtained. Existing Class 2 arrangements shall be assessed against the Nigerian incorporation, issuer licensing and service-provider approval requirements. Any continued access during assessment shall require the Bank's express interim permission and shall not confer a permanent exemption from those requirements. A person operating a Platform-Facilitated Peer-to-Peer Service at commencement shall apply for the approval required under Section 10 within the same period and may continue only on the same terms.

Section 55 Transition and Pilot Arrangements

55.1 The Bank may issue guidance, circulars and directions for the interpretation and implementation of these Regulations within its statutory mandate. Questions of classification shall be determined by economic substance and the applicable law. Interpretative guidance shall not dispense with an express legal prohibition or alter another competent authority's statutory functions.

55.2 In these Regulations, "shall" imposes an obligation and "may" confers a discretion. A reference to a licence or authorisation shall be read according to the relevant activity and conditions. Specific Deposit Money Token provisions shall govern the deposit-token matters they address. Statutory requirements shall prevail over an inconsistent provision of these Regulations.

Section 56 Publication Commencement and Application

56.1 The Bank shall publish these Regulations and specify its commencement date in the issuing instrument. The transition period in Section 54 shall run from that commencement date.

56.2 The Schedules form part of these Regulations. The Bank may prescribe forms, reporting channels, formats and implementation requirements consistently with these Regulations and applicable law. Existing obligations shall continue except to the extent expressly modified by a valid subsequent instrument.

SCHEDULE

Schedule 1 Licence and Authorisation Application Letter

The applicant or promoters shall write a letter to the Bank applying for AIP for a Naira-referenced Issuer Licence (Class 1), Foreign Currency Issuer Licence (Class 2) or Other Services Licence, or for an Other Services Authorisation or an Approval to Extend Permitted Activities where eligible. Identify the route, activities, tokens and incorporation status. Sections 7 to 9 and 11 govern the requirements. Proposed particulars may be supplied at AIP stage; certified incorporation documents and evidence of fulfilled conditions are required before final licensing.

Section A – Applicant Information

Full legal name or proposed name of applicant and names of promoters where unincorporated

CAC registration number if incorporated; otherwise state that Nigerian incorporation is proposed following AIP

Date and place of incorporation, or proposed Nigerian incorporation particulars

Registered address and principal place of business, or proposed Nigerian addresses

Contact person details (name, title, email, telephone)

Legal form (private limited company, public limited company, other – specify)

Proposed licence or authorisation category: Naira-referenced Issuer Licence (Class 1); Foreign Currency Issuer Licence (Class 2); Other Services Licence; Other Services Authorisation; or Approval to Extend Permitted Activities. Specify each proposed service and, for an Approval to Extend Permitted Activities, the Principal Licence held.

Name and proposed ticker symbol of the stablecoin

Section B – Ownership and Shareholding

Actual or proposed shareholders holding five per cent or more of issued or proposed share capital: full name, nationality, percentage holding and BVN for Nigerian individuals

Actual or proposed ultimate beneficial owners, including persons owning or controlling five per cent or more through any chain and persons otherwise exercising ultimate control

Actual or proposed organisational chart showing legal and beneficial ownership and control

Section C – Directors and Senior Management

Full names, nationalities, and positions of all proposed directors

Full names and positions of proposed Chief Executive Officer, Chief Compliance Officer, and Chief Risk Officer

Completed Fit and Proper Questionnaires for all directors, senior managers, controllers and significant shareholders identified in this application, using Schedule 2.

Section D – Business and Operational Information

Detailed three-year business plan

Proposed stablecoin design and stability mechanism

Proposed blockchain networks

Proposed reserve management strategy and proposed custodians

Description of smart contract architecture and controls

Smart contract audit reports

Section E – Financial Information

Source-of-funds evidence, proposed funding and evidence of deposits already made; before final licensing, evidence of applicable paid-up capital, capital deposit, RTGS transfer or permitted securities and lien under Sections 15 to 17

Audited financial statements for preceding two years or management accounts if incorporated for less than two years; for unincorporated applicants, opening financial projections and proposed funding evidence

Projected balance sheets, income statements, and cash flows for three years

Section F – Compliance Information

AML/CFT/CPF compliance programme document

KYC procedures manual

Transaction monitoring system description

Travel Rule compliance architecture

Proposed Chief Compliance Officer details and CV

Section G – Technical and Risk Management

Technology architecture diagram

Cybersecurity framework summary

Business continuity plan

Risk management framework document

Proposed wind-down plan

Section H – Disclosures

Completed Stablecoin Whitepaper (as per Schedule 5)

Draft terms and conditions for holders

Draft customer disclosure document

Proposed reserve attestation engagement letter from Approved Independent Auditor

Section I – Declarations

Declaration by the Chief Executive Officer and Chairman where appointed, or the promoters where unincorporated, that information is accurate and complete and applicable obligations are accepted; the incorporated applicant shall confirm adoption and compliance before final licensing

Evidence of payment of application fee

Additional Class 2 Licensed Issuer Information

Actual or proposed Nigerian incorporation, staffed principal office, ownership, local management and regulatory contact; reference currency and token design; distribution and redemption partners; reserve composition, custody, backing and holder protection; separate operational liquidity, accessibility and stressed Nigerian redemption capacity; Nigerian activity and cross-border/FX data; lawful freeze, burn, block and monitoring controls; continuity and wind-down; and systemic requirements where applicable. Complete and evidence final conditions before operations.

Additional Information for Other Service Applicants

Valid SEC licence and approved service scope for an Other Services Authorisation applicant; standalone non-security service scope for an Other Services Licence applicant; relevant principal licences; service-specific customer-asset safeguards, key management, reconciliation, conversion, settlement and customer-protection controls; and capital additional to applicable SEC requirements.

Independent Assessments

Submit paragraph 10A reports with the AIP application and paragraph 10B reports before final licensing. Each report shall be not more than six months old at submission. Include assessor qualifications, independence and conflicts declarations, remediation evidence and reasons for claimed inapplicability for the Bank's determination.

Schedule 2 Fit and Proper Questionnaire

The following information shall be supplied for every actual or proposed director, senior manager, controller and significant shareholder of an applicant or Licensee, in accordance with Section 18.

Part I – Personal Information

Full legal name; date of birth; nationality; country of primary residence; current and previous positions held in financial institutions or technology companies in the past ten (10) years.

Part II – Integrity Declarations

Have you ever been convicted of any criminal offence in any jurisdiction? If yes, provide full details.

Have you ever been the subject of any regulatory, disciplinary, or professional body investigation, proceeding, or sanction in any jurisdiction? If yes, provide full details.

Have you ever been a director, officer, or significant shareholder of a financial institution that was placed into insolvency, receivership, or administration? If yes, provide full details.

Have you ever been disqualified from serving as a director of a company in any jurisdiction? If yes, provide full details.

Are you currently subject to any criminal investigation, civil proceeding, or regulatory inquiry in any jurisdiction? If yes, provide full details.

Have you ever been subject to bankruptcy or insolvency proceedings, or are you currently insolvent? If yes, provide full details.

Part III – Financial Soundness

Do you have any unsatisfied court judgements against you in any jurisdiction? If yes, provide full details.

Declaration of personal net worth and sources of funds for any proposed investment in the applicant entity.

Part IV – Competence

Academic qualifications (certified copies of certificates to be provided).

Professional qualifications and memberships.

Summary of relevant experience in financial services, digital assets, technology, or related fields.

Part V – Independence (for proposed independent non-executive directors)

Description of any existing or proposed business, financial, personal, or other relationships with the applicant entity, its shareholders, or its management that may affect independence.

Part VI – Declaration

Signed declaration that all information provided is accurate and complete, and that the declarant accepts the obligation to notify the Bank promptly of any change in circumstances relevant to the Fit and Proper assessment.

Schedule 3 Fee Schedule

The following amounts are in Nigerian Naira. Application fees are non-refundable where indicated.

Application fee for Naira-referenced Issuer Licence (Class 1): ₦10,000,000 (non-refundable)

Application fee for Foreign Currency Issuer Licence (Class 2): ₦10,000,000 (non-refundable)

Annual renewal fee for Naira-referenced Issuer Licence (Class 1): ₦5,000,000

Annual renewal fee for Foreign Currency Issuer Licence (Class 2): ₦5,000,000

Examination fee: Actual cost of examination as assessed by the Bank

Fees for Other Services and activity-specific approvals

Fees for an Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities shall be as prescribed by the Bank.

Where an application includes a request for approval to operate or facilitate a Platform-Facilitated Peer-to-Peer Service under Section 10, the applicant shall pay:

a) the application fee applicable to the underlying Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities; and

b) any activity-assessment, systems-review, inspection or supervisory fee prescribed by the Bank for the proposed P2P Service.

A Licensee applying after the grant of its licence, authorisation or approval to add a Platform-Facilitated Peer-to-Peer Service to its approved scope shall pay the prescribed fee for a variation or extension of permitted activities.

Approval of a P2P Service shall not constitute, or attract a fee for, a separate licence category. Examination, technology validation, inspection and independent-review costs may be recovered at actual cost as assessed by the Bank.

The annual renewal or supervisory fee applicable to a Licensee approved to provide a P2P Service shall be as prescribed by the Bank.

Payment of a fee shall not dispense with any capital, liquidity, safeguarding, systems, reporting or other requirement imposed under these Regulations.

Fees for Other Services Licences, Other Services Authorisations and Approvals to Extend Permitted Activities shall be those prescribed by the Bank. No additional amount is specified in this Schedule.

The Bank may review applicable fees from time to time. A fee does not replace a capital or reserve requirement.

Schedule 4 CBN Reserve Deposit Account Agreement Prescribed Terms

The CBN Reserve Deposit Account Agreement between the Bank and each Class 1 Licensed Issuer shall contain the following terms, subject to Section 24 and applicable law. Class 2 operational-liquidity arrangements are governed by Sections 11 and 24.50 and do not require an agreement under this Schedule.

The Account shall be designated as "[Issuer Name] Stablecoin Reserve Deposit Account" and shall be clearly identified as held for the benefit of stablecoin holders in priority to all creditors of the Issuer.

Minimum balance shall be not less than twenty per cent (20%) of the Class 1 issuer's total Reserve Pool, calculated daily, or any higher percentage prescribed under Section 24.27. The denominator is the total Reserve Pool rather than only the face value of circulating tokens.

The Bank shall maintain real-time electronic access to Account balances and shall be entitled to query and receive transaction-level data in respect of the Account at any time.

Withdrawals from the Account may only be made with the prior written consent of the Bank, or pursuant to an instruction from a Special Purpose Administrator appointed under Sections 14.8 and 24.48, or to meet redemption obligations in a stress scenario approved in writing by the Bank.

The Account shall not bear interest.

In the event of insolvency of the Issuer, the Bank shall apply the balance of the Account exclusively to meet outstanding redemption obligations of stablecoin holders, in priority to all other claims.

Any higher Class 1 percentage prescribed under Section 24.27 shall be reflected in the account terms. The Account remains separate from the capital deposit under Section 17.

Schedule 5 Stablecoin Whitepaper Requirements

Every Licensed Issuer shall prepare and publish a Stablecoin Whitepaper prior to the issuance of any stablecoins. The Whitepaper shall be reviewed and approved by the Bank as part of the licensing process and shall contain the following mandatory sections:

Issuer Information: Full name of the issuer; registered address; directors and key management; regulatory status; corporate structure and ownership; financial standing; and contact details for holder enquiries.

Stablecoin Description: Name and ticker symbol; reference asset; peg mechanism; blockchain networks on which the stablecoin is issued; smart contract architecture, including the address(es) of deployed smart contracts; and a description of the minting, transfer, and redemption lifecycle.

Reserve Management: describe backing, eligible assets, allocation, custodians, segregation and concentration. For Class 1, disclose the ordinary 20% CBN Reserve Deposit, any valid higher percentage under Section 24.27, the additional 40% cash/HQLA minimum excluding that deposit, maturity limits, 30% per-bank limit and minimum three Deposit Money Banks. For Class 2, disclose reference-currency backing, the 40% cash/HQLA minimum, approved custody and concentration arrangements, and separate operational liquidity accessible for normal and stressed Nigerian redemptions. No fixed Class 2 domestic reserve share applies.

Rights of Holders: The absolute right of redemption at par value; the redemption timeline (maximum one Business Day); the redemption process, including how holders may initiate redemptions; the circumstances in which redemption may be suspended; the prohibition on interest and yield; and the treatment of holders in insolvency.

AML/CFT Framework: A high-level description of the AML/CFT programme, KYC requirements applied to users, transaction monitoring capabilities, Travel Rule compliance, and the mechanisms available to law enforcement and regulatory authorities.

Technology and Security: A description of the smart contract controls, including freeze, burn, and deny-listing capabilities; the cybersecurity framework; the audit history of the smart contracts; and the issuer's approach to smart contract upgrades.

Risk Factors: A frank and complete description of the material risks to which stablecoin holders are exposed, including reserve risk, technology risk, regulatory risk, liquidity risk, and counterparty risk.

Governance: Description of the board and management structure; key policies; and the process for making material changes to the stablecoin's design, reserves, or governance.

Regulatory Status: A statement of the licences and authorisations held by the issuer; the applicable regulatory framework; and the identity of the Bank as the primary regulatory authority.

Disclosures: A statement that the stablecoin is not a bank deposit and is not covered by the NDIC deposit guarantee scheme; a statement that holding the stablecoin does not entitle the holder to interest, yield, or any form of investment return; and a risk warning approved by the Bank.

Nigerian Activity and Risk Disclosures: material Nigerian use cases, Nigerian-linked circulation and transaction measures, cross-border and FX considerations, concentration, redemption, operational, reserve and regulatory risks, and circumstances in which the Bank may restrict business or suspend or revoke the licence.

Class 2 Additional Disclosures: identity and Nigerian regulatory status of the Class 2 Licensed Issuer; approved Nigerian distribution and redemption providers; reference currency; legally enforceable redemption rights; applicable FX arrangements; reserve and liquidity disclosures; material licence conditions; and a clear statement that CBN licensing does not constitute a guarantee or endorsement.

Schedule 6 Reserve Attestation Report Format

Every Reserve Attestation Report submitted under Section 24 shall be prepared by the Approved Independent Auditor in the following standard format:

Report Title: Reserve Attestation Report – [Issuer Name] – [Month and Year]

Engagement Summary Name of the Approved Independent Auditor; engagement scope; date of attestation; reference date (the date as at which reserves are measured).

Stablecoins in Circulation Total number of stablecoin tokens in circulation as at the reference date; methodology for calculating circulating supply (e.g., total minted minus total burned); comparison with the preceding month's circulating supply.

Reserve Pool Summary Aggregate naira value of the Reserve Pool as at the reference date; comparison with the total naira value of stablecoins in circulation; reserve coverage ratio (Reserve Pool / Circulating Supply x 100%); statement of compliance or non-compliance with the full reserve backing and additional 2% overcollateralisation requirement.

Reserve Composition Detail A detailed breakdown of the Reserve Pool by asset type, showing for each category: asset type; naira value; percentage of total Reserve Pool; name of custodian institution; account reference; and maturity date (for time-limited instruments such as Treasury Bills).

CBN Reserve Deposit and Class 2 Operational Liquidity: for Class 1, report balance, reserve percentage, compliance with 20% or valid higher minimum, breaches and approved access. For Class 2, report separate liquidity resources, prescribed requirements, accessibility, stress results, replenishment and shortfalls; confirm no double counting as reserves or capital.

Reserve Concentration Analysis: identify banks and custodians, assets held and reserve share. For Class 1, include the CBN deposit in the denominator and confirm the 30% per-bank limit and three-bank minimum in addition to the CBN. For Class 2, confirm approved arrangements and limits under Sections 24.35 to 24.39 without assuming domestic allocation. Report Section 24.36 investment-counterparty limits where applicable.

Cash and HQLA Liquidity Minimum: identify qualifying cash and HQLA, values, reserve percentages and non-cash maturities. Confirm the 40% minimum, six-month ceiling and shorter limits under Section 24.12. For Class 1, exclude the CBN deposit from counted assets. For Class 2, report reference-currency reserve liquidity separately from operational liquidity.

Segregation Confirmation Statement by the Approved Independent Auditor confirming that reserve assets are held in accounts that are legally and operationally segregated from the issuer's operational funds, based on confirmation received from each custodian institution.

Reserve Leverage Confirmation: confirm compliance with the encumbrance prohibition on the basis of enquiries and custody evidence. Identify any permitted liquidity transaction under Section 24.34, its approval and compliance with safeguards.

Auditor's Conclusion A positive or qualified conclusion by the Approved Independent Auditor as to whether, as at the reference date, the Reserve Pool meets the requirements of these Regulations. Any qualifications shall be described in detail.

Management Response (where applicable) Where the Approved Independent Auditor has issued a qualified conclusion, the issuer's management shall provide a written response setting out the steps being taken to remedy the identified deficiency.

For Class 2, state original denomination, Naira-equivalent methodology, reference-currency liabilities and FX exposure; confirm Section 24.30 compliance and report operational liquidity under Sections 11 and 24.50. Report applicable bank, custody and investment-counterparty limits and exceptions without a local reserve percentage.

Illustrative reserve composition for a Class 1 Stablecoin

Component	Requirement	Eligible assets	Section
CBN Reserve Deposit	Not less than 20% of the Reserve Pool	Cash in the Reserve Deposit Account at the Bank	24.25–24.27
Cash and high-quality liquid assets	Not less than 40% of the Reserve Pool, in addition to and excluding the CBN Reserve Deposit	Cash at Deposit Money Banks; qualifying Treasury Bills, FGN bonds, overnight reverse repos and OMO bills with a residual maturity of not more than six months	24.12
Other Eligible Reserve Assets	The balance of the Reserve Pool (up to 40%)	Treasury Bills (≤90 days); FGN bonds (≤180 days); naira deposits at Deposit Money Banks; SEC-regulated naira money market funds (≤10% of reserves)	24.28
Reserve buffer	Not less than 2% of the par value of stablecoins in circulation, from own funds	Held within the segregated Reserve Pool; released only with the Bank's approval	24.4, 24.52
Concentration	Not more than 30% per Deposit Money Bank; at least three Deposit Money Banks; not more than 40% per investment counterparty	Applies across all reserve components, with the CBN Reserve Deposit included in the denominator	24.35–24.38

Schedule 7 Supervisory Reporting Templates

General Reporting Rules

1. Reports under this Schedule shall be submitted electronically through the supervisory reporting channel designated by the Bank, in the format, file structure, taxonomy, and data dictionary prescribed by the Bank. Unless otherwise stated, reports shall preserve the original currency and stablecoin denomination and provide the required naira equivalent.

2. Each report shall identify the reporting entity, reporting period, stablecoin, issuer, distribution partner, relevant wallet or account identifiers, source system, and responsible officer, and shall contain sufficient information to permit reconciliation across issuer, VASP, bank, payment, FX, custodian, and on-chain records.

3. The Bank may prescribe validation rules, unique transaction identifiers, duplicate controls, data-quality attestations, and resubmission requirements. Reporting entities shall retain the underlying records supporting each return and make them available for supervisory review.

4. Routine supervisory returns shall be submitted to the Bank. Where substantially identical data are required by the SEC or another competent authority, the Bank may establish coordinated or interoperable reporting arrangements to minimise duplicative submissions.

5. Suspicious Transaction Reports shall be filed with the NFIU under Section 26.9 and its prescribed process. Individual STR contents shall not be reproduced in routine CBN returns except where lawfully required.

6. Material incidents and changes shall be notified under Section 20 and the applicable reserve, redemption and sanctions duties. Routine monthly returns shall not replace immediate, 24-hour or other event reporting.

Monthly Regulatory Report — Required Data Fields

Part A — Stablecoin and Market Activity

1. Total stablecoin tokens in circulation (opening, closing, peak, and average for the month), including Nigerian-linked circulation where available and the methodology used for attribution.

2. Total value of stablecoins in circulation at month-end, reported in original denomination and naira equivalent.

3. Total value and number of stablecoins minted and redeemed during the month, including the issuer, distribution partner, and redemption channel.

4. Total number of active Nigerian users or wallet addresses, with methodology and limitations disclosed.

5. Transaction volume and value by direction (Nigerian-originating, Nigerian-receiving, domestic loop, and cross-border), counterparty category, and purpose.

6. Fiat leg and stablecoin leg of relevant transactions, including NGN amount, foreign-currency amount, stablecoin amount, exchange/conversion rate, and transaction identifier.

7. Concentration metrics, including top counterparties, largest user holdings, distribution-partner concentration, and material exposure to any single issuer or stablecoin.

Part B – Reserve and Redemption Metrics

8. Reserve value, coverage, asset class, currency, custodian, maturity, liquidity and breaches. Identify 40% cash/HQLA compliance and maturities. For Class 1, exclude the CBN deposit from counted HQLA and report bank limits and number of banks. For Class 2, report separate operational

liquidity, accessibility in Nigeria, expected and stressed redemptions, buffers, replenishment and prescribed-requirement compliance.

9. CBN Reserve Deposit balance where applicable and percentage of total Reserve Pool.

10. Redemption requests received, processed, pending, rejected, suspended, average processing time, and peak redemption demand, including the redemption route used for Class 2 Stablecoins.

11. Reserve attestations, material qualifications, custodian changes, and legal or operational segregation exceptions.

Part C – AML/CFT/CPF and Sanctions Metrics

12. AML/CFT alerts generated, escalated, closed, and outstanding; STR count filed with the NFIU; sanctions screening hits; and material typologies identified, without disclosing individual STR contents unless lawfully required.

13. Number of wallet addresses frozen, blocked, deny-listed, or otherwise restricted pursuant to lawful regulatory or law-enforcement action.

Part D – Operational, Technology and Consumer Metrics

14. Platform outages, cybersecurity incidents, smart-contract incidents, recovery performance, and material business-continuity events.

15. Complaints received, categorised by type, value, status, and resolution time; material unresolved complaints; and consumer-impact events.

Part E – Regulatory and Governance Metrics

16. Material changes to ownership, governance, key management, regulatory status of the issuer or its group, distribution partners, custodians, reserve arrangements, or operational capabilities.

17. Certification by the Chief Executive Officer and Chief Compliance Officer, or the responsible senior officers of another Licensee, that the return is complete and accurate and identifies known exceptions.

Part F – Platform-Facilitated Peer-to-Peer Service Metrics

A Licensee approved to operate or facilitate a Platform-Facilitated Peer-to-Peer Service shall report the following information for the reporting period:

18. total number and value of P2P transactions, disaggregated by Regulated Token, transaction type, customer category and transaction status;

19. the Naira, other fiat or payment leg and the corresponding virtual-asset leg of each reportable transaction, including the transaction identifier, payment or settlement reference, wallet address or account identifier, transaction hash, exchange or conversion rate and time of settlement;

20. P2P transaction volumes and values by:

a) purchase, sale or exchange;

b) domestic or cross-border transaction;

c) Class 1 Stablecoin, Class 2 Stablecoin or other approved Regulated Token;

d) customer and counterparty category;

e) payment or settlement channel; and

f) direction of flow;

21. Naira inflows and outflows associated with P2P transactions, including the relevant Nigerian banking, payment or settlement channel and the financial institution through which the payment leg was effected;

22. the number and value of transactions involving conversion between Naira and a Class 2 Stablecoin or other foreign-currency value, including the authorised dealer, transaction purpose, supporting documentation and compliance with applicable approval conditions;

23. customer and counterparty information, including the number of active P2P customers, new customers, business users identified under Section 10.3.5, customer risk categories and concentration by customer or counterparty; matching, escrow and settlement information, including transactions placed in escrow, released, returned, cancelled, reversed, failed, incomplete or pending at the end of the reporting period;

24. the number and value of disputed, fraudulent, anomalous or unauthorised transactions, together with complaints received, amounts affected, resolution status and average resolution time;

25. transaction-monitoring alerts, sanctions-screening alerts, wallet-monitoring alerts and suspicious or anomalous P2P patterns identified, without reproducing the contents of individual Suspicious Transaction Reports except where lawfully required;

26. transactions involving third-party, nominee, mule, fictitious or improperly attributed payment accounts or wallets, including the action taken by the Licensee;

27. transactions involving unhosted wallets or another VASP, including the number and value of such transactions and compliance with the applicable Travel Rule and counterparty due-diligence requirements; domestic and cross-border P2P activity by jurisdiction, corridor, token, settlement channel and transaction purpose;

28. concentration by customer, counterparty, Regulated Token, wallet, financial institution, payment channel, settlement channel and jurisdiction;

29. breaches or attempted circumvention of transaction, customer, volume, geographic, foreign-exchange, documentation or other limits imposed by the Bank;

30. material outages, reconciliation exceptions, escrow failures, settlement failures, fraud events, cybersecurity incidents and other operational incidents affecting the P2P Service; and

31. such additional transaction-level, periodic, event-driven, real-time or near-real-time information as the Bank may prescribe.

Information submitted under this Part shall be sufficient to reconstruct and reconcile each P2P transaction across its virtual-asset and fiat, payment or settlement legs. Direct customer-to-customer settlement, outsourcing, offshore processing or the use of distributed-ledger technology shall not reduce the Licensee's reporting obligations.

Class 2 Reserve Redemption and Cooperation Information

Each Class 2 Licensed Issuer shall report reference currency, reserve coverage and liquidity, original denomination and Naira equivalents, Nigerian-linked circulation, redemption volumes and routes, material delays or restrictions, separate operational-liquidity resources, Nigerian accessibility, stress results, buffers, replenishment and shortfalls, and continued compliance with licence, information-access and cooperation conditions.

Other Services and DMT Returns

Other-service providers shall report service-specific volumes, values, assets controlled, safeguarding and reconciliation, capital, operational incidents, complaints and compliance. DMT Issuing Banks shall report issuance, outstanding deposit liabilities, reconciliation, redemption, transfers, settlement and other data under Section 47. No stablecoin reserve form shall misclassify a DMT as a separately reserve-backed issuer token.

Reporting Calendar

In accordance with Section 20.2, the Reporting Calendar below consolidates the returns, frequencies and deadlines in these Regulations and prevails over any inconsistent timeline elsewhere. Stress and systemic returns follow Sections 17 and 24. Other routine frequencies and formats shall be prescribed by the Bank.

Return or notification	Frequency	Deadline	Recipient	Public or confidential	Section
Daily reserve reconciliation	Daily	End of each Business Day (records available to the Bank)	Retained; available to the Bank	Confidential	20.13, 24.5
Monthly regulatory return (Parts A to E of this Schedule)	Monthly	As prescribed by the Bank	Bank	Confidential	20.8
Reserve attestation	Monthly	Fifteen Business Days after month-end	Bank and published	Public	20.7, 24.42
Class 2 provider transaction returns	Monthly	Ten Business Days after month-end	Bank	Confidential	20.9
Top ten Class 2 counterparties; complaints register	Quarterly	With the quarterly return	Bank	Confidential	20.8, 20.9
Incident notification	Event-driven	Within 24 hours of awareness; immediately for serious threats	Bank	Confidential	20.4
Incident follow-up report	Event-driven	Within 72 hours of initial notification	Bank	Confidential	20.5

Return or notification	Frequency	Deadline	Recipient	Public or confidential	Section
Suspension of redemptions	Event-driven	Immediately and within one hour; no longer than 48 hours without approval	Bank and public notice	Public notice	23.6, 23.7
Class 1 Reserve Deposit shortfall	Event-driven	Same Business Day; restoration plan under 24.5.3	Bank and public notice	Confidential	24.5.2
Capital shortfall	Event-driven	Immediately; restoration plan within ten Business Days	Bank	Confidential	17.5
Use of freeze, block or burn functions	Event-driven	Within 24 hours	Bank; NFIU where relevant	Confidential	26.18.4
New network, bridge or smart-contract change	Event-driven	At least 30 days in advance	Bank	Confidential	26.20.2
Changes to published customer information	Event-driven	Disclosed within 48 hours	Public	Public	20.13
Penetration test results	Annual and on completion	Within 30 days of completion	Bank	Confidential	20.13, 37.10
AML/CFT/CPF independent audit findings	Annual	Within 30 days of completion	Board and Bank	Confidential	26.2.5

Return or notification	Frequency	Deadline	Recipient	Public or confidential	Section
Annual renewal declaration	Annual	By 31 January	Bank	Confidential	20.12
Audited financial statements with reserve opinion	Annual	Within four months of financial year-end	Bank	Confidential	20.7, 24.45
Suspicious transaction reports	Event-driven	Promptly and within 24 hours of forming suspicion under Section 26.9.1, through the NFIU's prescribed channel	NFIU	Confidential	26.9
Platform-Facilitated Peer-to-Peer Service Return under Part F	Monthly, or more frequently where prescribed by the Bank	Within ten Business Days after month-end, or within such shorter period as the Bank may prescribe	Bank	Confidential	10.8, 20.12 and Schedule 7, Part F
Material P2P incident, control failure, limit breach, material reconciliation exception, significant fraud event or loss of supervisory visibility	Event-driven	In accordance with Section 20.4; immediately where the event presents a serious threat	Bank; NFIU where separately required	Confidential	10.8, 20.3–20.5

Schedule 8 CBN and SEC Delineation Matrix

This Schedule illustrates the allocation of regulatory responsibility under Section 4. It shall be read subject to Section 4 and to any Harmonised Implementation Framework adopted under the Presidential Executive Order on Virtual Assets Coordination, 2026.

Part A – Delineation Matrix

Activity or Instrument	CBN	SEC	Allocation Rule and Notes
Issuance of fiat-referenced stablecoins (Class 1 Stablecoins; Class 2 Stablecoins)	Lead	–	Payment instrument redeemable at par with no return. Prudential, reserve, redemption and foreign-exchange oversight by the Bank.
Deposit Money Tokens	Lead	–	A bank liability. Prudential supervision by the Bank; deposit insurance by the NDIC.
Payments, transfers, remittances and merchant acceptance using Non-Security Virtual Assets	Lead	–	Payment-system and money-transfer activity.
Custodial Virtual Asset Payment Wallets, Virtual Asset Payment Gateway Services and Virtual Asset Stored-Value Facilities	Lead	–	Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities, according to the applicant's status (Section 9.2).
Naira or foreign-currency conversion to and from stablecoins (on-ramps and off-ramps)	Lead	Joint where on a digital asset exchange	The foreign-exchange and payment leg is regulated by the Bank. Where the conversion takes place on an SEC-licensed exchange, the SEC regulates the trading venue and the Bank authorises the payment or foreign-exchange service.
Custody of stablecoins and other value held for payment purposes	Lead	–	Safeguarding of payment value.
Custody of Security Virtual Assets	–	Lead	SEC digital asset custodian regime.
Custody of virtual assets solely for trading, brokerage or investment purposes	Only where a payment function is performed	Lead	Becomes a Non-Security Virtual Asset Payment Activity where the custodian also performs a payment function listed in Section 4.9.

Activity or Instrument	CBN	SEC	Allocation Rule and Notes
Offering, issuance and trading of Security Virtual Assets, tokenised securities and investment tokens	Payment leg only	Lead	Investments and Securities Act, 2025, section 357. The Bank regulates only the cash or stablecoin settlement leg (Section 4.4).
Virtual asset exchanges, brokers and platform operators	Other Services Authorisation for non-security services	Lead	Dual approval for dual activity. The lead supervisor is determined by the predominant activity (Section 4.3).
Yield-bearing tokens, tokenised money market funds and staking-return products	–	Lead	A return to holders makes the product an investment. It is prohibited as a payment stablecoin (Section 13.3).
Unbacked crypto-assets	Payment services	Trading and investment	Classification to be confirmed by the Council. Interim default: trading and investment business with the SEC; payment use with the Bank.
Payment use of a stablecoin listed on an SEC-licensed platform	Lead for payment use	Lead for listing and trading	Listing does not authorise payment use (Section 4.10). Payment use requires an Approved Virtual Asset Payment Instrument and a CBN licence or authorisation (Section 9.13).
Reserve-asset management by Licensed Issuers	Lead	Fund level	The Bank sets reserve rules. The SEC regulates any money market fund in which reserves are invested.
Banks' exposures to, and services for, VASPs	Lead	–	Prudential treatment and provision of bank accounts.
AML/CFT/CPF supervision	Own Licensees	Own licensees	The NFIU receives STRs. The Travel Rule applies to all VASPs. Joint inspections where an entity is licensed by both authorities.

Part B – Classification indicators

The following indicators point to a Security Virtual Asset: the token carries a right to profit, interest, dividend or a share of revenue; its value is designed to fluctuate with the performance of an enterprise or a pool of assets; it is marketed as an investment; it confers governance or ownership rights in an enterprise; or redemption is not at par. Any one of these indicators points to a Security Virtual Asset.

The following indicators point to a Non-Security Virtual Asset: a fixed par value; an unconditional right of redemption; no return to the holder; and use primarily for payment, settlement or transfer of value.

Part C – Licensing & authorisation routes for other services

Applicant	Route	Scope	Capital	Key Provisions
Person licensed, registered or approved by the SEC	Other Services Authorisation	Non-security services specified in Section 9.1, including a Platform-Facilitated Peer-to-Peer Service where expressly approved by the Bank under Section 10. SEC-regulated listing, trading, brokerage and other capital-market activities remain subject to SEC regulation.	₦1,000,000,000, additional to SEC capital under Sections 16.1 and 16.2, or such higher amount as the Bank may prescribe.	Sections 6.2(d), 9.1, 9.3, 10, 14.11 and 14.12
Financial institution licensed by the Bank (Deposit Money Bank, Payment Service Bank, mobile money operator, payment solution service provider, international money transfer operator or switch)	Approval to Extend Permitted Activities	Non-Security Virtual Asset Payment Activities only; no issuance, exchange, trading or SEC activities	Principal Licence capital plus ₦1,000,000,000 under Section 16.1, not counted towards Principal Licence capital (Sections 9.4A.4 and 16.3).	Sections 6.2(e), 9.4A, 14.11, 14.12, 16.3, 18.7.
Any other person	Other Services Licence	Any service in Section 9.1	₦1,000,000,000 (Section 16.1)	Sections 6.2(c), 9.2, 9.4 to 9.9
Deposit Money Bank tokenising deposits	Approval under Part 10	Issuance of Deposit Money Tokens	Banking licence capital	Part 10
Financial institution licensed by the Bank, including a Deposit Money Bank, Payment Service Bank, mobile money operator, payment solution service provider, international money transfer operator or switch	Approval to Extend Permitted Activities	Non-Security Virtual Asset Payment Activities within the scope of the institution's Principal Licence. This may include a Platform-Facilitated Peer-to-Peer Service involving Approved Virtual Asset Payment Instruments where expressly approved under Section 10. It does not authorise general virtual-asset exchange, brokerage, dealing, trading or another activity within SEC's mandate.	Principal Licence capital plus ₦1,000,000,000 under Section 16.1, not counted towards Principal Licence capital, or such higher amount as the Bank may prescribe.	Sections 6.2(e), 9.4A, 10, 14.11, 14.12, 16.3 and 18.7

Part B – Classification indicators

Applicant	Route	Scope	Capital	Key Provisions
Any other person	Other Services Licence	Any service specified in Section 9.1, including a Platform-Facilitated Peer-to-Peer Service where expressly approved by the Bank under Section 10. The approval shall specify the Regulated Tokens, customers, transaction types, settlement arrangements, geographic scope and other applicable conditions.	₦1,000,000,000 under Section 16.1, or such higher amount as the Bank may prescribe.	Sections 6.2(c), 9.1, 9.2, 9.4–9.9 and 10

Platform-Facilitated Peer-to-Peer Services: The Bank shall not grant a separate licence category solely for a Platform-Facilitated Peer-to-Peer Service. A person may provide such service only where:

a) it holds an Other Services Licence, Other Services Authorisation or Approval to Extend Permitted Activities, as applicable; and

b) the Bank has expressly approved Platform-Facilitated Peer-to-Peer Services within the scope of that licence, authorisation or approval.

An approval permitting another service under Section 9 shall not, by itself, authorise a Platform-Facilitated Peer-to-Peer Service. An Approval to Extend Permitted Activities shall cover only Approved Virtual Asset Payment Instruments and shall not authorise general virtual-asset exchange, brokerage, dealing, trading or investment activity.

Annex: Documents to be Submitted with an Application

Submit the following documents to the extent applicable. Identify proposed arrangements and outstanding AIP conditions and explain claimed inapplicability. Sections 7 to 9 and 11 and Schedule 1 govern requirements and stages; paragraph 10A reports accompany the AIP application and paragraph 10B reports precede final licensing. No final licence shall be granted without Nigerian incorporation and fulfilled conditions.

1. Corporate and Licensing Documents

a) Completed application letter.

b) Certified incorporation and constitutional documents where incorporated; otherwise draft memorandum and articles of association and proposed Nigerian incorporation particulars, with certified documents before final licensing.

c) Actual or proposed ownership and beneficial ownership structure, including controllers, proposed shareholders and persons of significant control.

d) Details of any principal licences, registrations or approvals, including any licence issued by the Securities and Exchange Commission or a foreign competent authority, where applicable.

e) Fit and proper questionnaires for actual or proposed directors, senior management, controllers and significant shareholders.

f) Evidence of source of funds.

g) Source-of-funds and proposed funding information; confirmation of deposits already made and full capital evidence, including RTGS or permitted custody and lien evidence, before final licensing.

h) Three-year business plan, financial projections and implementation roadmap.

i) Audited financial statements or management accounts where available; opening financial projections and funding evidence for an unincorporated applicant.

j) Evidence of payment of the prescribed application fee.

2. Product and Customer Documentation

a) Whitepaper and customer terms and conditions.

b) Customer risk disclosures.

c) Customer complaints management and dispute resolution procedures.

3. Governance, Risk and Compliance Documentation

a) Corporate governance framework and policies, in draft for promoters and adopted by the constituted board before final licensing.

b) Accounting policies and procedures.

c) Internal control framework.

d) Enterprise risk management framework.

e) AML/CFT/CPF policies and procedures.

f) Travel Rule compliance framework and supporting architecture.

4. Technology and Operational Documentation

a) Technology and systems architecture.

b) Cybersecurity, information security and key management policies.

c) Smart contract audit reports, where applicable.

d) Penetration testing and vulnerability assessment reports, where applicable.

e) Operational readiness assessment covering the mandatory readiness requirements prescribed by the Bank.

5. Reserve Management and Stablecoin Documentation

a) Reserve composition policy.

b) Reserve segregation arrangements.

c) Custody arrangements for Reserve Assets.

d) Reconciliation procedures.

e) Liquidity management framework.

f) Redemption policy and procedures.

g) Nigerian legal opinion addressing asset protection, reserve segregation and holder priority rights.

h) Details of the proposed independent auditor.

6. Commercial, Outsourcing and Third-Party Arrangements

a) Banking agreements.

b) Custody agreements.

c) Distribution agreements.

d) Agency agreements.

e) Outsourcing agreements and third-party service arrangements.

Platform-Facilitated Peer-to-Peer Service Documentation

An applicant seeking approval to operate or facilitate a Platform-Facilitated Peer-to-Peer Service shall submit:

i. a detailed description of the proposed P2P Service, identifying:

a) the Regulated Tokens proposed to be supported;

b) customer and counterparty categories;

c) transaction types;

d) whether the service is domestic or cross-border;

e) the proposed geographic scope;

f) the proposed order-display, matching, escrow, payment, transfer, clearing, reconciliation, settlement, verification and dispute-resolution functions; and

g) any agent, distributor, technology provider or outsourced service provider involved;

ii. a process-flow and systems-architecture diagram showing the complete transaction lifecycle and the interaction between:

a) the customer and counterparty;

b) the P2P platform;

c) any escrow arrangement;

d) the virtual-asset wallets or accounts;

e) the Naira, fiat, banking, payment or settlement channels; and

f) relevant VASPs, financial institutions and service providers;

iii. the proposed customer identification, verification, customer due-diligence, ongoing-monitoring and access-control framework, including controls for:

a) matching a customer's verified identity, name and Bank Verification Number with the relevant payment

b) attributing every account, wallet and transaction to the appropriate customer and counterparty; and

c) preventing the use of third-party, nominee, mule, fictitious or improperly attributed accounts or wallets;

iv. the criteria and procedures for identifying customers conducting P2P activity as a business, including the applicable enhanced due diligence, transaction limits, escalation and regulatory-reporting arrangements;

v. the transaction-monitoring, blockchain-analytics, sanctions-screening, fraud-prevention and suspicious-activity detection framework applicable to the P2P Service;

vi. the proposed controls for order matching, rate display, transaction verification, escrow, release of virtual assets, payment confirmation, failed transactions, cancellation, reversal and dispute resolution;

vii. the safeguarding, segregation, reconciliation and key-management arrangements applicable where the applicant controls or escrows customer virtual assets or otherwise has Control of customer assets;

viii. the reconciliation methodology for linking each virtual-asset leg to its corresponding Naira, fiat, payment or settlement leg, including unique transaction identifiers and exception-management procedures;

ix. details of each proposed Nigerian banking, payment or settlement channel, including agreements or term sheets with participating financial institutions or payment service providers;

x. where conversion between Naira and a Class 2 Stablecoin or other foreign-currency value is proposed:

a) the relevant foreign-exchange approval sought;

b) the proposed authorised dealer;

c) permitted transaction purposes;

d) documentation requirements;

e) transaction and customer limits; and

f) foreign-exchange and balance-of-payments reporting arrangements;

xi. the P2P AML/CFT/CPF, sanctions and Travel Rule framework, including the treatment of:

a) transactions between customers of the applicant;

b) transactions involving another VASP;

c) transactions involving an unhosted wallet;

d) cross-border P2P activity; and

e) suspicious or anomalous P2P patterns;

xii. the proposed data model, record-keeping arrangements and regulatory-reporting architecture demonstrating the applicant's ability to reconstruct and report each P2P transaction and its virtual-asset and fiat, payment or settlement legs;

xiii. customer terms, disclosures and risk warnings specifically addressing:

a) the role of the provider;

b) matching and settlement;

c) escrow and safeguarding;

d) fees, spreads and exchange or conversion rates;

e) transaction suspension, cancellation and reversal;

f) failed, disputed, fraudulent and erroneous transactions; and

g) material risks associated with the P2P Service;

xiv. the complaints, fraud-claim, dispute-resolution and escalation procedures applicable to the P2P Service;

xv. business-continuity, incident-response and orderly-wind-down arrangements specific to the P2P Service, including the treatment of transactions in progress and virtual assets held in escrow;

xvi. the proposed transaction, customer, volume, concentration, token, geographic, settlement-channel and cross-border limits;

xvii. an independent assessment of the design and operating readiness of the P2P Service, covering technology, cybersecurity, customer identification, transaction monitoring, escrow, safeguarding, reconciliation, settlement, reporting, fraud controls and business continuity; and

xviii. any other information, testing result, legal opinion, assurance, undertaking or operational demonstration required by the Bank.

7. Business Continuity and Exit Arrangements

a) Business continuity plan.

b) Disaster recovery plan.

c) Wind-down and orderly exit plan.

8. Class 2 Stablecoin-Specific Information

a) Reference currency, reserve backing and custody, Nigerian redemption arrangements, and separate operational liquidity, accessibility, stress capacity, buffers, replenishment and reporting.

b) Nigerian Class 2 issuer, foreign group or sponsor, approved distribution and market access, supervisory access and cooperation, and allocation of responsibilities without substitution for Nigerian issuer obligations.

9. Additional Information

a) Any other information, document, assessment, report or undertaking that the Bank may require for the purpose of evaluating the application.

10. Independent Assessments (Section 7.7)

10A. To be submitted with the application:

a) Capital requirements.

b) Corporate governance and risk management.

c) Business conduct and customer protection.

d) AML/CFT/CPF control systems, including the AML/TF/PF risk assessment.

e) Independent Nigerian legal opinion on the segregation of the Reserve Pool and holder-priority arrangements (see Part E of this Annex and Section 24.46).

10B. To be submitted and found satisfactory before the Bank grants the Issuer Licence under Section 8.6:

a) Management of the Reserve Pool, including the operational readiness of reserve, custody and reconciliation arrangements.

b) Technology risk management, including the independent smart contract security audits required by Section 37.5 and penetration testing.

c) Payment security management.

d) Business continuity management.

e) Redemption testing.

For an applicant seeking approval to provide a Platform-Facilitated Peer-to-Peer Service, the pre-licensing assessments under this paragraph shall include operational testing of customer attribution, payment-account verification, transaction matching, escrow and release controls, reconciliation of the virtual-asset and payment legs, transaction monitoring, regulatory reporting, dispute handling and supervisory data access.

For further information
please contact:

The Director, Payments System
Policy Department
Central Bank of Nigeria

NOVEMBER 2026