



ANTI-FINANCIAL CRIMES POLICY

Version Control

Title	Anti-Financial Crimes Policy
Category	Policy Document
Version	3.5
Approving Authority	Board of Directors

DOCUMENT OWNERSHIP & CREATION RECORD

VERSION	DESCRIPTION	APPROVED BY	DATE
1.0 – AML	Anti-Money Laundering Policy was created and approved	Board	April 2018
1.0 – ABC	Anti-Bribery & Corruption Policy was created and approved	Board	December 2018
2.0 – ABC	Reviewed Anti-Bribery & Corruption Policy to comply with ISO 37001	Board FAC	May 2022
3.0	Merged Anti-Bribery & Corruption Policy, Anti-Money Laundering Policy and Policy Governance Framework	EXCO	May 2023
3.1	Updated Honorarium provisions	Board FAC	December 2023
3.2	Updated Gift Threshold	EXCO	March 2024
3.3	Re-named Anti-Financial Crimes Policy, updated policy review period, due diligence procedures, definition of PEPs, regulatory reporting	EXCO	June 2025
3.4	Revised the review period of the AFC Policy from every three (3) years to every two (2) years, based on the feedback from the Board Finance & Audit Committee. This includes edits to pages 26, 29 and 34.	Board FAC	July 15, 2025
3.4	Board Approval	Board	July 28, 2025
3.5	Adoption of the Securities and Exchange Commission (SEC) (Capital Market Operators AML/CFT/CPF Regulations, 2022 and inclusion of Proliferation Financing requirements.	EXCO	March 27, 2026

POLICY SEGMENTATION

A. POLICY SECTION – ANTI-BRIBERY & CORRUPTION POLICY	4
1. Introduction	5
2. Scope and Applicability	6
3. Anti-Bribery Policy Statement	6
4. Definitions	7
5. Anti-Bribery Management System	8
6. Bribery Risk Assessment	10
7. Reporting Structure, Policy Governance and Management Review	11
8. Maintenance of Records and Documented Information	14
9. Measures to Prevent and Combat Fraud, Bribery and Corruption by InfraCredit and Beneficiaries of its Guarantee Whether Directly or Indirectly	14
10. Integrity Due Diligence	15
11. Investigations into Allegations of Misconduct and Integrity Violations by InfraCredit or Third Parties	16
12. The Investigative Process	18
13. Whistleblowing Policy and Procedural Guidelines	19
14. Sanctions	21
15. Treatment of Politically Exposed Persons and Measures to Prevent and Combat Fraud, Bribery and Corruption with Government or Public Officials	21
16. Measures to be Taken in Dealing with Public Officials	21
17. Charitable Donations	22
18. Gifts and Hospitality	22
19. No Intermediaries	23
20. Performance Evaluation	24
21. Reporting Requirements	25
22. Amendments	25
23. Communication	25
24. Availability	26
25. Changes to the Policy	26
26. Policy Review	26
B. POLICY SECTION – AML/CFT/CPF POLICY	27
1. Introduction	27
2. Anti-Money Laundering, Combating the Financing of Terrorism and Combating Proliferation Financing	28
3. Reporting	32
A. Appendices	35

POLICY SECTION A

ANTI-BRIBERY & CORRUPTION POLICY

Policy Statement

InfraCredit provides local currency guarantees to enhance the credit quality of debt instruments to finance creditworthy infrastructure assets in Nigeria that conform with its eligibility criteria and attracts investments from pension funds, insurance firms and other long-term investors thereby deepening the Nigerian debt capital markets. This Policy sets forth our commitment to preventing and detecting money laundering, bribery and corruption wherever it may arise and is derived from the comprehensive Anti-Financial Crimes Policy.

A bribe means directly or indirectly giving anything of value to any person including a public official to influence an official act, secure an improper advantage, or obtaining or retain the business of any person or entity, or induce a person to perform a function or activity improperly, or act in violation of a duty. Corruption means the abuse of illegitimate use of office for financial or non-financial private gain and includes bribery, soliciting or receiving facilitation payments and kickbacks, money laundering, embezzlement, misappropriation, fraud and other related offences. Facilitation payment means the payment of a small, unofficial amount to advantage a public official without a written receipt to secure or expedite a routine government action.

This Policy outlines our standards for interactions with all stakeholders. We take reasonable measures to ensure that all interactions with stakeholders with whom we work demonstrate respect and regulations, such as those set under 'Scope and Applicability – 2.4', in the comprehensive policy.

We are committed to doing business with high integrity and complying with applicable laws and regulations, internal policies and procedures. We adhere to the laws and regulations applicable in Nigeria where we operate.

We conduct business ethically and transparently. We prohibit all forms of bribery, corruption and other behaviour that could cause or appear to cause improper influence. We prohibit the making of facilitation payments.

We will not offer, promise or provide any inducements, such as payments or other things of value or perceived value to obtain an improper advantage in any of our business transactions or interactions.

We will not select someone to provide services, to directly or indirectly, obtain an improper advantage or improperly influence or encourage a decision or action. Neither will we offer indirect inducements, such as those made to family members.

We must have legitimate business reasons for everything we do. Stakeholders may only be engaged to provide services for which we have a legitimate business need that is defined and documented in advance, and for which such persons are appropriately qualified. Meals, drinks, travel, entertainment and accommodation can only be offered, provided or paid for in connection with a legitimate business reason, and only to the actual participants, and never to influence or personally benefit third parties, and always following local requirements.

We ensure that all interactions with stakeholders are transparent and accurately documented. The purpose and appropriateness of any payment, gift, hospitality, entertainment and similar arrangement

must be clear. Books, records and accounts must accurately and fairly reflect all transactions and dispositions in reasonable detail.

Failure to follow the principles set out above and in the comprehensive Policy may result in disciplinary action, up to and including termination for employees of InfraCredit. In addition, breaches of antibribery or anticorruption laws can have severe financial and reputational consequences for InfraCredit. Stakeholders who are involved and implicated in the breach risk imprisonment and personal fines.

Compliance with this and associated Policies will be monitored through the Board, Finance & Audit Committee, Board Risk and Capital Committee, Top Management, Chief Risk Officer, and Head of Compliance, annual reviews, and internal audits.

1. INTRODUCTION

- 1.1. At Infrastructure Credit Guarantee Company (**InfraCredit** or the **Company**), we believe that corporate bribery is not just illegal but unethical. The Company and its management are thus committed to conducting our business operations in an ethical and honest manner with due compliance with all relevant statutes and applicable standards. The Company's reputation is built upon a foundation of integrity and our operations must continue to maintain that same level of stellar conduct and legal compliance.

THE ORGANISATION AND STAKEHOLDERS

- 1.2. InfraCredit is an investment institution providing local currency guarantees to enhance the credit quality of debt instruments to finance creditworthy infrastructure assets in Nigeria that conform with its eligibility criteria and attracts investments from pension funds, insurance firms and other long-term investors thereby deepening the Nigerian debt capital markets.
- 1.3. The Company operates in a wide range of sectors including agriculture, water distribution, power, transportation, renewable energy, ICT/telecom, social infrastructure amongst others. Given the public nature of these sectors, the Company works in close proximity with several government institutions and regulators.
- 1.4. The relevant stakeholders are capital investors, public sector and regulators, investment clients etc. These stakeholders expect the highest level of disclosure and transparency in order to enhance value for money and return on investment whilst reducing the risk of fraud and corruption.
- 1.5. Notwithstanding, each stakeholder comes with unique expectations that must be uniquely addressed and identified.
 - a. Our shareholders expect full compliance with the terms of this Policy, as failure to do so may ultimately affect dividends where the Company is subjected to sanctions from regulators and loss of business
 - b. Capital investors, both current and prospective, are more likely to invest and place trust in the Company if a robust anti-bribery policy is implemented, to ensure that the normal course of business is not tainted with corrupt practices.
 - c. Our employees play a dual role, as they can directly affect compliance with the Policy. The efficiency of anti-bribery mechanisms itself relies on the personal integrity of employees and their willingness to abide by them. In turn, failure to comply with the Policy by all or some employees may result in prosecution, a major restructuring that impacts the workforce, and sanctions that impact the ability to work, not just in the Company, but in larger investment space.
 - d. Our investment clients want to be sure that our services are not tainted with corruption
 - e. Our business associates rely on our assurance that no corrupt act will affect business relations or lead to reputational damage.

- f. Ultimately, the public is the victim of corrupt acts, as it destroys trust, and leads to higher prices and lower quality of services.

2. SCOPE AND APPLICABILITY

- 2.1. This Anti-Bribery and Corruption Policy (the Policy) is applicable only to bribery and corruption.
- 2.2. The Policy applies to all staff, temporary, contractual or permanent, regardless of role or level of seniority including all managers and directors of the Company as well as consultants, agents and any other third party which act in the Company's name (together referred to as Company Officials). Without prejudice to the foregoing, the Policy applies to all other persons or entities which either receive (either directly or indirectly) InfraCredit funding for their own use, or benefit from its credit guarantees, or are responsible for the deposit or transfer of InfraCredit funding or proceeds of debt instruments guaranteed by InfraCredit (whether or not they are beneficiaries of such proceeds), or take or influence decisions regarding the use of InfraCredit funding or the proceeds of debt instruments guaranteed by InfraCredit.
- 2.3. The Company has established, documented therein, implemented, maintains, and continually reviews and, where necessary, improves its anti-bribery management system, including the processes needed and their interactions, in accordance with the requirements of this document. This anti-bribery management system contains measures designed to identify and evaluate the risk of, and to prevent, detect and respond to, bribery.
- 2.4. This Policy is also designed to comply with applicable statutory and regulatory obligations as stipulated by the:
 - 2.4.1. OECD Convention on the Fight against Corruption of Public Officials dated 17 December 1997
 - 2.4.2. OECD Recommendation for further Combating Bribery of Foreign Public Officials dated 9 December 2009.
 - 2.4.3. Economic and Financial Crimes Commission Establishment Act 2004;
 - 2.4.4. Corrupt Practices & Other Related Offences Act 2000;
 - 2.4.5. Securities and Exchange Commission (Capital Market Operators Anti-Money Laundering and Combating the Financing of Terrorism) Regulations 2022
 - 2.4.6. Constitution of the Federal Republic of Nigeria (as amended)
 - 2.4.7. Advance Fee Fraud and Other Fraud Related Offences Act 2006;
 - 2.4.8. Money Laundering (Prohibition) (Amendment) Act 2022;
 - 2.4.9. Miscellaneous Offences Act Cap M17 LFN 2004;
 - 2.4.10. Code of Conduct Bureau and Tribunal (Amendment) Act 1993;
 - 2.4.11. Nigerian Extractive Industries Transparency Initiative Act 2007;
 - 2.4.12. Freedom of Information Act 2007;
 - 2.4.13. Fiscal Responsibility Act 2010;
 - 2.4.14. Penal Code (Northern States) Federal Provisions Act Cap P3 LFN 2004;
 - 2.4.15. Criminal Code Act Cap C38 LFN 2004;
 - 2.4.16. Banks and Other Financial Institutions (Amendment) Act 2020;
 - 2.4.17. United Kingdom Bribery Act 2010;
 - 2.4.18. United States Foreign Corrupt Practices Act of 1977;
 - 2.4.19. Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994; and
 - 2.4.20. Wolfsberg Anti-Bribery and Corruption (ABC) Compliance Programme Guidance.
- 2.5. This Policy is designed to prevent and combat fraudulent and corrupt misconduct and practices that may occur in connection with the Company's activities.
- 2.6. This Policy is designed to comply with the ISO37001 Standards.

3. ANTI-BRIBERY POLICY STATEMENT

- 3.1. InfraCredit is built on trust and integrity as perceived by its stakeholders. An important element of trust and integrity is ensuring that InfraCredit conducts its business in accordance with the Code of Ethics and Business Conduct as adopted by InfraCredit and in compliance with applicable laws, rules and regulations.
- 3.2. InfraCredit has a “zero tolerance” policy towards bribery and corruption and is committed to the highest levels of anti-bribery and corruption compliance and therefore requires management and all staff to adhere strictly to the provisions of this policy in its interaction with stakeholders and third parties.
- 3.3. The Executive Management shall establish, maintain and review this anti-bribery Policy that prohibits bribery and requires compliance with anti-bribery laws that are applicable to the Company and is appropriate to the purpose of the Company. This Anti-Bribery Policy provides a framework for setting, reviewing and achieving anti-bribery objectives and includes a commitment to satisfy anti-bribery management system requirements. This Policy encourages raising concerns in good faith, or on the basis of a reasonable belief in confidence, without fear of reprisal.
- 3.4. This Policy is committed to continual improvement of the antibribery management system and details the authority and independence of the anti-bribery compliance function as well as explains the consequences of not complying with the antibribery policy.

4. DEFINITIONS

In this Policy, unless the context otherwise requires:

- 4.1. **Head of Compliance** means any member of the Company appointed by the Executive Management Committee to fill that role;
- 4.2. **Bribe** means directly or indirectly giving anything of value to any person including a Public Official for the purpose of influencing an official act, securing an improper advantage, or obtaining or retaining the business of any person or entity, or inducing a person to perform a function or activity improperly, or act in violation of a duty.
- 4.3. **“Anything of value”** can include, but is not limited to:
 - 4.3.1. monetary gains, upgrade to first class airfare, sponsoring school tuition for family members, gifts, hospitality, etc.
 - 4.3.2. providing cars for personal use, doing business with a company owned or controlled by a Public Official, or hiring a family member of a Public Official.
- 4.4. **Bribery** means the soliciting, offering, promising, giving, accepting or receiving of a Bribe;
- 4.5. **Charitable Contribution** means a cash or kind contribution made to non-profit associations or organizations for social, educational, environmental and cultural benefit;
- 4.6. **Chief Risk Officer** means the corporate executive responsible for identifying, analysing and mitigating internal and external events that could threaten the Company (or equivalent position);
- 4.7. A **Coercive Practice** is impairing or harming, or threatening to impair or harm, directly or indirectly, any part of the property of the party to influence improperly the actions of a party;
- 4.8. A **Collusive Practice** is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;
- 4.9. A **Corrupt Practice** is the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;
- 4.10. **Corruption** means the abuse or illegitimate use of office for financial or non-financial private gain, and includes Bribery, soliciting or receiving Facilitation Payments and Kickbacks, money-laundering, embezzlement, misappropriation, fraud and other related offences;
- 4.11. **Facilitation Payment** means the payment of a small, unofficial amount or advantage to a Public Official without a written receipt in order to secure or expedite a routine government action. For example, making “grease” payments to arrange or speed up a service like issuing a

- passport or visa, or obtaining approvals and licenses, or to avoid prosecution by authorities or penalties.
- 4.12. A **Fraudulent Practice** is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation;
- 4.13. An **Obstructive Practice** is:
- 4.13.1. deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making a false statement to investigators in order to materially impede an investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or
- 4.13.2. intended to materially impede the exercise of InfraCredit's contractual rights of audit or access to information.
- 4.14. **Integrity Violation** is any act which violates InfraCredit's zero tolerance policy on bribery, corruption and fraud.
- 4.15. **Issuer** means a company incorporated in Nigeria to whom the Company has provided a credit guarantee.
- 4.16. **Kickbacks** mean payments made in return for a business favour or advantage.
- 4.17. **Money Laundering** means the process employed to disguise the illegal origin and/or illegitimate ownership of an asset which is acquired by criminal activities.
- 4.18. **Prohibited Acts** include:
- 4.18.1. payments, or grant of any other advantage, to government officials, beyond what is required by law or local regulations, to obtain a permit, license, or other necessary approval.
- 4.18.2. payments or grant of any other advantage to government officials in order to avoid an inspection, influence the findings of an inspection, or avoid a fine.
- 4.18.3. authorization or request to any Company Official or third party to pay bribes to anyone (including government officials) or receive bribes from anyone.
- 4.18.4. overlooking any activity by Company Officials or third parties acting on the Company's behalf that you suspect might conflict with this Policy.
- 4.19. **Public Official** means any local or international (i) person engaged or employed in any capacity in the public service of any government entity or any entity that is partially or wholly owned or controlled by the government, (ii) officer of a political party, or (iii) political candidate.
- 4.20. **Sanctionable Practices** include a bribe or bribery, a fraudulent practice, a collusive practice, a coercive practice, an obstructive practice, Integrity Violation and Prohibited Act as defined above.
- 4.21. **Sanctions List** means the list stating the persons/organisations the Company is precluded from dealing with, as published by the Executive Management Committee.
- 4.22. **Shell Bank** means a financial institution which does not have a physical presence in any country.

5. **ANTI-BRIBERY MANAGEMENT SYSTEM**

- 5.1. The Company has established, implemented and will continually review to improve its anti-bribery management system, including the processes needed and their interactions, in accordance with International best standards and the requirements of ISO 37001. This anti-bribery management system contains measures designed to identify and evaluate the risk of, and to prevent, detect and respond to, bribery. This admits that it is not possible to completely eliminate the risk of bribery, and no anti-bribery management system will be capable of

- preventing and detecting all bribery, however this anti-bribery management system will mitigate bribery risk to the greatest extent.
- 5.2. This Policy:
- 5.2.1. identifies and evaluates the risks of and how to prevent, detect and respond to bribery and corruption.
 - 5.2.2. sets out the framework for the process of handling investigations into alleged bribery, corruption or possible Integrity Violations.
 - 5.2.3. defines how such investigations are to be handled, sets out the persons responsible for such investigations and defines sanctions and consequences of material breach.
 - 5.2.4. sets out the mode of review and improvement of the risks and processes identified above.
- 5.3. InfraCredit and such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees must take all appropriate measures to prevent, report and combat fraud, bribery and corruption and Sanctionable Practices as defined in Section 4 of the Policy.
- 5.4. InfraCredit, its directors and its Company Officials have a duty to ensure that the funding received by the Company is used for the purposes for which it was deployed, with due attention to considerations of economy and efficiency and without regard to political or other non-economic influences or considerations.
- 5.5. Each director, member of management of an Issuer or other entity funded by, or whose debt instrument is guaranteed by the Company, has a duty to make arrangements to ensure that the funding, or the proceeds of such guaranteed debt instrument is used for the purposes for which it was deployed or for which the debt instrument was issued, with due attention to considerations of economy and efficiency and without regard to political or other non-economic influences or considerations. This Policy constitutes an important element of such funding or guarantee arrangements.
- 5.6. This Policy covers fraud, bribery and corruption in the diversion of the proceeds of debt instruments guaranteed by InfraCredit, funds granted to InfraCredit or granted by InfraCredit for eligible expenditures, as well as fraud, bribery, and corruption for the purpose of influencing any decision as to the use of the proceeds of debt instruments guaranteed by InfraCredit, and funds granted to InfraCredit or granted by InfraCredit.
- 5.7. This Policy applies to the procurement or execution of contracts for goods, works or services on behalf of the Company.
- 5.8. The Company shall hold mandatory training programs annually to ensure that Company Officials and third parties who act on behalf of the Company, understand all applicable anti-bribery and corruption laws and act in compliance with those laws. These training programs shall be developed by the Compliance Department to target specific risks faced by the Company and the country where InfraCredit operates. It is imperative that all Company Officials attend these training programs.
- 5.9. The Company has established this anti-bribery management system with objectives at relevant functions and levels.
- 5.10. The objectives of the anti-bribery management should be measurable, achievable, monitored objectives and is communicated and updated as appropriate. The objective is to achieve a zero tolerance of bribery and a "No" to any form of corruption.
- 5.11. The objective of this system is in line with the ISO Standard 6.2 and shall be measured by the Company's Annual Risk Assessment. Its objective will be updated from time to time as there are changes to the business and its processes.
- 5.12. Management shall continually monitor the objectives of the Company through its Management review at the Executive Meeting.

- 5.13. The Management System shall continually be communicated during anti-bribery trainings and onboarding sessions to staff. In addition, all staff shall be made to read and acknowledge this system and abide by the system.
- 5.14. The Company shall retain information on the antibribery management system which has:
- what will be done;
 - what resources will be required;
 - who will be responsible;
 - when the objectives will be achieved;
 - how the results will be evaluated and reported;
 - who will impose sanctions or penalties.

6. BRIBERY RISK ASSESSMENT

- 6.1. In this Policy, a three-tier risk model is adopted for the evaluation and assessment of bribery risk. This is High Risk, Medium Risk and Low Risk. Despite this model, it is reiterated that InfraCredit has zero tolerance to bribery and corruption and regardless of the assessment given to any identified risk, it is committed to ensuring absolute compliance in its interactions with its stakeholders and third parties.
- 6.2. The identified risks are:
- 6.2.1. Bribery including Fraudulent Practices, Collusive Practices, Obstructive Practices, Integrity Violations and Prohibited Acts;
 - 6.2.2. Money Laundering;
 - 6.2.3. Kickbacks;
 - 6.2.4. Corruption; and
 - 6.2.5. Facilitation Payments.
- 6.3. The risk assessment is conducted in four categories according to the nature of the Company's business, its stakeholders and its activities. These categories are Government, Capital Investors, Clients, Third Parties (Procurement and Services).
- 6.4. Interactions with government officials and regulators for approvals and investments may involve Money Laundering, Facilitation Payments, Corruption and Kickbacks. Given the pervasive lack of transparency and accountability within government institutions, extra measures are put in place in this Policy to control the risks identified herein. Government and Public Officials are therefore deemed **High Bribery Risk**.
- 6.5. Interactions with Capital Investors may involve Collusive Practices, Bribery and Integrity Violations in the grant of funds and debt instruments to InfraCredit. However, Capital Investors come from highly regulated sectors and the international community which place a demand of transparency on their activities as well, hence, the bribery risk can be controlled. Capital Investors are deemed **Low Bribery Risk**.
- 6.6. Interactions with Investment Clients may involve Bribery, Collusive Practice, Facilitation Payment and Kickbacks from such Clients to employees and members of the Company in the diversion of the proceeds of debt instruments guaranteed by InfraCredit, funds granted to InfraCredit or granted by InfraCredit for eligible expenditures, as well as fraud, bribery, and corruption for the purpose of influencing any decision as to the use of the proceeds of debt instruments guaranteed by InfraCredit, and funds granted to InfraCredit or granted by InfraCredit. However, given the restricted sectors of the investment and the Company's level of scrutiny, transparency and accountability required in investing in infrastructure projects, the bribery risks identified can be controlled. Investment Clients are deemed **Low Bribery Risk**.
- 6.7. Interactions with Third Parties may involve Collusive Practices, Bribery, Corruption in the procurement and execution of contracts for goods, works and services. Such Third Parties are deemed **Medium Bribery Risk**.

- 6.8. The Company undertakes to regularly, at least on annual basis, conduct Anti-bribery risk assessment(s), which shall:
- a) identify the bribery risks the Company might reasonably anticipate,
 - b) analyse, assess and prioritize the identified bribery risks;
 - c) evaluate the suitability and effectiveness of the organization's existing controls to mitigate the assessed bribery risks.
- Notwithstanding the above, the Company shall conduct an assessment, following a restructuring, change in scope of activities, or compliance with an audit or regulatory requirements, before the annual review is due.
- 6.9. In carrying out the risk assessment, a six-step approach will be followed:
- 6.9.1 Step 1: Ensuring Top-Level Commitment and Oversight**
- Top-level management is key to effective risk management. The board and senior management will provide leadership and accountability to drive adequate and continuing risk assessment, ensuring that the process does not falter or lose quality
- 6.9.2 Step 2: Planning, Scope and Mobilisation**
- A planning team will be set up (of internal or external personnel) who will prepare the basics of the risk assessment process. They will appoint a project leader, define interested parties, their needs and expectations, allocate team responsibilities and authorities, identify information sources, draft the plan for risk assessment, and communicate the plan and requirements to those involved in the risk assessment process.
- 6.9.3 Step 3: Information Gathering**
- Comprehensive data on inherent/potential bribery risks to which the Company could be exposed by the nature and location of its activities will be created. Opportunities for anti-bribery will also be identified
- 6.9.4 Step 4: Identifying Bribery Risks and Opportunities of Anti-bribery**
- The risk factors that increase the company's exposure to bribery risk will also be identified and examined.
- 6.9.5 Step 5: Evaluation and Prioritisation of Risks**
- Considering their likelihood and severity, the various risks will be categorised into High, Medium, and Low
- 6.9.6 Step 6: Using Output of Risk Assessment to develop Operational Controls**
- Overall, the results of the risk assessment will be applied to review the Anti-Bribery Policy and associated policies towards improving operational controls and programs, developing new ones where needed, and introducing modifications or additions as deemed necessary.
- 6.10. The Company shall retain appropriate documented information as evidence of the methods and results. The organization shall evaluate the anti-bribery performance and the effectiveness and efficiency of the anti-bribery management system.
- 6.11. The Company shall establish criteria for evaluating its level of bribery risk, which shall take into account the organization's policies and objectives. The bribery risk assessment shall be reviewed:
- a) on an annual basis so that changes and new information can be properly assessed based on timing and frequency defined by the organization;
 - b) in the event of a significant change to the structure or activities of the Company. The Company shall retain documented information that demonstrates that the bribery risk assessment has been conducted and used to design or improve the anti-bribery management system.

7. REPORTING STRUCTURE, POLICY GOVERNANCE AND MANAGEMENT REVIEW

- 7.1. The Reporting structure of the Company is as follow, from top: the Board, Finance & Audit Committee, Board Risk and Capital Committee, Top Management (MD/CEO and Senior Executives), Chief Risk Officer and the Head of Compliance.
- 7.2. The Board and Management of the Company shall be responsible for:
 - 7.2.1. ensuring that the Policy is maintained, so far as applicable, in line with the principles and guidelines of relevant international, local financial institutions and the ISO 37001;
 - 7.2.2. conducting periodical reviews of the Policy such as internal audit process, to test its effectiveness and update the Policy in line with new developments in relevant laws and leading practice;
 - 7.2.3. ensuring all Company Officials are aware of the Policy and adopt the procedures stipulated by the Policy in preventing and combating fraud, bribery, corruption and other Sanctionable Practices that may occur in connection with their activities;
 - 7.2.4. ensuring that the organization's strategy and anti-bribery policy are aligned;
 - 7.2.5. requiring that adequate and appropriate resources needed for effective operation of the anti-bribery management system are allocated and assigned; and
 - 7.2.6. exercising reasonable oversight over the implementation of the organization's anti-bribery management system by top management and its effectiveness.
- 7.3. Board Oversight
 - 7.3.1. The Board has a supervisory role and oversight regarding the Company's Anti-Bribery Management System and this Policy. It is responsible for ensuring the adequacy, effectiveness and implementation of the system and should receive regular information regarding the performance of the system.
 - 7.3.2. The Board through the Finance & Audit Committee or such other committee nominated by the Board shall consider reports on compliance with internal policies, programs and procedures. It is also required to review and evaluate, at least annually, the reports on fraud, bribery and corruption produced by the Compliance Officer and the actions taken by senior management in relation to these reports.
- 7.4. Board Risk and Capital Committee

The Board Risk and Capital Committee shall:

 - 7.4.1. Review the Policy, compliance programmes and the ABAC Reporting Officer/Compliance Officer's reports and make recommendations to the Board.
 - 7.4.2. Monitor InfraCredit's performance and compliance with the Policy.
 - 7.4.3. Review breaches of the Policy and actions taken by senior management/executives to resolve such issues.
- 7.5. Top Management/ Executive Oversight

The Managing Director/Chief Executive Officer shall:

 - 7.5.1. effectively oversee the implementation of the Policy across the Company;
 - 7.5.2. ensure that there is a right "tone at the top" on adherence to the Policy;
 - 7.5.3. put in place appropriate policies and controls to give effect to the Policy and ensure that they are effective; and
 - 7.5.4. allocate any other required roles and responsibilities to appropriate staff to monitor and ensure compliance.

Senior Executives shall:

 - 7.5.5. ensure that the requirements of the Policy are incorporated into divisional processes;
 - 7.5.6. be accountable for delivering the outcome of processes and procedures contained in this Policy in their particular area of responsibility;
 - 7.5.7. support the Head of Compliance in the execution of the responsibilities of his/her positions and review his/her reports;

- 7.5.8. review at regular intervals the status of actions from previous management and board reviews as well as changes in external and internal issues relevant to the Policy and the anti-bribery system;
- 7.5.9. review the performance of the anti-bribery system including trends in non-conformities and corrective actions, monitoring and measurement results, audit results, reports of bribery, investigations and the nature and extent of the bribery risks faced by the Company;
- 7.5.10. ensure effectiveness of actions taken to address bribery risks;
- 7.5.11. seek opportunities for continual improvement of the anti-bribery system; and
- 7.5.12. ensure adequate report is made to the Risk and Capital Committee and the Board.
- 7.6. The Head of Compliance
 - 7.6.1. The Head of Compliance shall be given overall responsibility within the organisation for the establishment and maintenance of effective systems and controls consistent with the requirements of the relevant anti-bribery and anti-corruption laws and regulations and the provisions of the Policy.
 - 7.6.2. The Head of Compliance shall work jointly together and be the contact persons between InfraCredit and the regulators.
 - 7.6.3. The Head of Compliance shall have the relevant competence, authority and independence within the organisation and have access to resources and information sufficient to enable him/her carry out stipulated responsibilities and shall deal with all disclosures confidentially and make decisions on the reporting of suspicious activity.
 - 7.6.4. The Head of Compliance must be familiar and ensure compliance with all legislations and regulations to combat anti-bribery and anti-corruption as listed under Section 2.
 - 7.6.5. The roles and responsibilities of the Head of Compliance include:
 - 7.6.6. Report suspicious persons/entities and activities to the Executive Committee of the Company which will provide report to the Risk & Capital Committee of the Board. Where necessary, suspicious persons/entities and activities are reported to law enforcement agencies in Nigeria including the Economic and Financial Crimes Commission and the Independent Corrupt Practices Commission and other relevant authorities in the appropriate manner;
 - 7.6.6.1. Develop and review, at least annually, anti-bribery and anti-corruption (ABAC) processes and procedures and provide enhancement recommendations, as appropriate, to the Risk and Capital Committee;
 - 7.6.6.2. Monitor and review existing and new sanctions as introduced and amended and determine how they affect InfraCredit;
 - 7.6.6.3. Review, identify and update potential risk areas in the identification of Sanctionable Practices;
 - 7.6.6.4. Ensure the internal audit function of InfraCredit regularly conducts a test as to the adequacy, completeness and effectiveness of the ABAC compliance programme;
 - 7.6.6.5. Provide a heightened awareness of key ABAC issues and techniques; develop and administer a comprehensive training programme for all relevant staff on ABAC including mandatory training for new employees.
 - 7.6.6.6. Serve as a liaison officer between InfraCredit and relevant regulatory authorities and also as a contact person for all employees on ABAC and Sanctionable Practices related issues;
 - 7.6.6.7. Prepare reports for the Risk and Capital Committee on ABAC and Sanctionable Practices related issues;
 - 7.6.6.8. Develop and maintain InfraCredit's ABAC compliance and report register; and

7.6.6.9. Continuously monitor, review and vet suspicious transaction reports from relevant staff.

8. MAINTENANCE OF RECORDS AND DOCUMENTED INFORMATION

RECORDS ON INVESTORS AND ISSUERS

- 8.1. InfraCredit must preserve all necessary records of investors, Issuers and third parties for a minimum of six (6) years (or longer if requested in specific cases) following the completion of all business relationships. Documents shall be preserved in accordance with the IT Policy of the Company.
- 8.2. The Company shall establish controls to ensure that documents are available and suitable for use, where and when it is needed, and it is adequately protected from loss of confidentiality, integrity and improper use etc.
- 8.3. This requirement includes all due diligence documents, details of transactions and all other necessary documents relating to business transactions between InfraCredit and Investors/Issuers.
- 8.4. Records must be easily accessible to the ABAC Reporting Officer/Compliance Officer and regulators on a timely basis.
- 8.5. For the control of documented information, as it relates to the distribution, preservation of legibility, access, retrieval and use, storage and preservation, version control, retention and disposition, the Information Technology & Data Protection Policy of the Company shall administer it in accordance with this Management System.
- 8.6. A breach of this requirement may cause InfraCredit to be liable to sanctions in accordance with the provisions of national and international laws and regulations related to anti-bribery and anticorruption.

OTHER RECORDS

- 8.7. All records of:
 - 8.7.1. suspicious transactions filed with regulators;
 - 8.7.2. Receipt of anti-bribery policy by personnel;
 - 8.7.3. Policies, procedures and controls of the anti-bribery system;
 - 8.7.4. Bribery risk assessment results;
 - 8.7.5. Anti-bribery training provided;
 - 8.7.6. Measures taken to implement the anti-bribery system;
 - 8.7.7. Results of monitoring, investigating or auditing carried out;
 - 8.7.8. Approvals and records of gifts, hospitality, donations and similar benefits given and received; and
 - 8.7.9. The actions and outcomes of concerns raised in relation to any weakness of the anti-bribery management system or incidents of attempted, suspected or actual bribery must be retained for a minimum of six (6) years after the filing of such reports. InfraCredit must provide these records to the regulators whenever they are legally required to do so.

9. MEASURES TO PREVENT AND COMBAT FRAUD, BRIBERY AND CORRUPTION BY INFRA CREDIT AND BENEFICIARIES OF ITS GUARANTEES WHETHER DIRECTLY OR INDIRECTLY

InfraCredit (either directly or indirectly) will:

- 9.1. Take all appropriate measures to prevent fraud, bribery and corruption in connection with the use of funding from InfraCredit, or the proceeds of debt instruments guaranteed by the Company including (but not limited to):
 - 9.1.1. adopting appropriate fiduciary and administrative practices and institutional arrangements to ensure that the funding from InfraCredit or proceeds of debt

instruments guaranteed by InfraCredit is used only for the purposes for which it was given or raised and also to ensure the easy detection of Sanctionable Practices.

- 9.1.2. monitoring systems and controls through internal and external audit;
- 9.1.3. complying with the Policy where applicable in line with any professional obligations;
- 9.1.4. discouraging conflicts of interest and maintaining interest registers;
- 9.1.5. ensuring procedures for selection and training of directors and employees support the selection of honest and competent individuals;
- 9.1.6. having a clear corporate policy direction in line with the Policy to act as a deterrent to potential wrong doers and that encourages others to pass on concerns over possible fraud or corruption;
- 9.1.7. ensuring that all third parties (either directly or indirectly) receive a copy of this Policy and are made aware of and adhere to its contents;
- 9.1.8. immediately report any allegations of fraud and corruption in connection with the use of funding from InfraCredit or the proceeds of debt instruments guaranteed by InfraCredit. Within two (2) days of receipt of an allegation, the Investigative Officer (as herein defined) shall inform the Chief Executive Officer, the Chief Risk Officer and/or the Board that an allegation has been made and will ensure that any individual or company connected to the allegation is also informed of the allegation;
- 9.1.9. if it is determined (after having followed the investigation procedure set out in this Policy) that a Company Official or other person has engaged in corrupt, fraudulent, collusive, coercive or obstructive practices in connection with the use of InfraCredit funding or proceeds of debt instruments guaranteed by InfraCredit, InfraCredit will take timely and appropriate action in accordance with the provisions of this Policy;
- 9.1.10. include such provisions in any agreements with third parties as may be required to give full effect to this Policy, including (but not limited to) provisions (i) requiring such third party to abide by this Policy, (ii) requiring such third party to permit InfraCredit's representatives to inspect all of their accounts and records and other documents relating to the project required to be maintained pursuant to the agreement and to have them audited by, or on behalf of, InfraCredit, and (iii) requiring the termination of any guarantees provided by InfraCredit, and/or the restitution by such third parties of any amount of any funding from InfraCredit with respect to which fraud and corruption has occurred; and
- 9.1.11. cooperate fully in any investigation into allegations of fraud and corruption in connection with the use of the proceeds of any debt instrument guaranteed by InfraCredit, or of funding from InfraCredit.

10. INTEGRITY DUE DILIGENCE

- 10.1. The Company shall consistently work to ensure the buy-in of Directors, Employees, Issuers and other third parties and ensure that they recognize the need to promote ethical business practices and good governance consistent with international standards as part of their credit and investment decisions.
- 10.2. The Company shall conduct Integrity Due Diligence on all Issuers and other entities or persons which receive funding either directly or indirectly from the Company or benefit from its credit guarantees. The Company shall be guided by the following general principles in analysing integrity issues relating to its capital raising, funding, guarantee, and investment decisions:
 - 10.2.1. adequate "know-your-customer" procedures to ensure identification of beneficial ownership provided that the Company shall conduct corporate searches on corporate bodies to determine the ultimate beneficial owners and where customers are individuals, details of identification, passport photograph, name, place and date of birth, gender and address must be obtained;

- 10.2.2. close scrutiny of parties that have been convicted of or are under investigation for serious crimes, investigated or sanctioned by a regulatory body or appearing on a Sanctions List by the Executive Management Committee;
- 10.2.3. close scrutiny of parties involved in civil litigation involving allegations of financial misconduct;
- 10.2.4. close scrutiny of Politically Exposed Persons consistent with the recommendations of the Financial Action Task Force;
- 10.2.5. identification of mitigants and enforcement of covenants that address integrity risks; and
- 10.2.6. on-going monitoring of integrity risks through portfolio management.

11. INVESTIGATIONS INTO ALLEGATIONS OF MISCONDUCT AND INTEGRITY VIOLATIONS BY INFRA CREDIT OR THIRD PARTIES

INTRODUCTION

- 11.1. The policy and the procedures set out in this section of this Policy are intended to be used as guidance in the conduct of investigations into Integrity Violations involving InfraCredit, its Company Officials or third parties. InfraCredit requires that all instances of suspected bribery, corruption and fraud be investigated thoroughly and where appropriate referred to the relevant authorities.

GENERAL

- 11.2. The Board shall nominate a person to be appointed as an Investigative Officer (the "Investigative Officer") for the purposes of investigations into Integrity Violations and misconduct by the Company in its dealings or third parties, who shall report to the relevant Head of Investigation (the "Head of Investigation") who shall also be nominated by the Board.
- 11.3. Any investigation into Integrity Violations and misconduct by the Company, Company Officials or third parties shall be carried out in accordance with this Policy.
- 11.4. The Investigative Officer shall be the initial point of contact for allegations of Integrity Violations and misconduct, reporting to the Head of Investigation.
- 11.5. The purpose of an investigation by the Investigative Officer is to examine and determine the veracity of allegations of Integrity Violations and misconduct for submission to the relevant Head of Investigation.
- 11.6. The Investigative Officer shall maintain objectivity, impartiality and fairness throughout the investigative process and conduct its activities competently and with the highest levels of integrity. In particular, the Investigative Officer shall perform its duties independently from the day-to-day operations of InfraCredit and shall be free from improper influence and fear of retaliation. The Investigative Officer may use such internal or external resources as may be considered necessary to carry out the investigation.
- 11.7. If the Investigative Officer has any real perceived, or apparent conflict of interest in an investigation, he or she shall declare such actual or potential conflict to the Head of Investigation.
- 11.8. Disclosure of conflicts of interest by the Investigative Officer in relation to an investigation shall be made promptly upon discovery and before any investigative action is taken. Any action to manage the conflict of interest shall be in writing.
- 11.9. Actions to address conflicts of interest may include, but are not limited to, exclusion from an investigation, and limits of access to case records and information.
- 11.10. If the subject of any investigation perceives that the Investigative Officer has not declared a conflict of interest in the investigation, or that a conflict of interest has not been managed appropriately, the subject of the investigation may request a review of the matter by the Head of Investigation.

- 11.11. The Investigative Officer shall assess allegations and conduct investigations under these procedures promptly and thoroughly and recommend the administrative action to be taken.
- 11.12. The principal responsibilities of the Investigative Officer are:
 - 11.12.1. to serve as the initial point of contact for all alleged incidents of Sanctionable Practices, bribery and corrupt practices;
 - 11.12.2. to conduct independent and objective investigations (using such internal or external resources as they may determine appropriate) of Sanctionable Practices, money-laundering and financing of terrorism;
 - 11.12.3. to provide investigative findings, which shall be dealt with as stipulated in these procedures;
 - 11.12.4. to report the findings of any such investigation; and
 - 11.12.5. to investigate allegations of misconduct by Company Officials involving Sanctionable Practices or abuse (theft, waste, or improper use of InfraCredit's assets, either committed intentionally or through reckless disregard), in accordance with this Policy.
- 11.13. The Investigative Officer shall ensure that all information and records associated with an investigation, including the identity of parties that are the subject of the investigation and of parties providing testimony or evidence, are kept confidential and under adequate physical, electronic and procedural controls. Each Investigative Officer shall ensure that the circulation of information regarding an investigation is only to those with a need-to-know. Depending on the nature of the case, the Investigative Officer may disclose certain evidence to the subject of an investigation in a manner that considers the need to protect whistle-blowers and witnesses.
- 11.14. Only the Investigative Officer, the Chief Risk Officer and the senior management of InfraCredit (if not the subject of the case and having not declared an actual or potential conflict of interest) may have access to information and records in relation to each case and may determine whether such information and records may be shared unedited or redacted with other parties. Information and records may only be shared unedited or redacted with other parties if the Board is satisfied that their document management systems are adequate to protect such information.
- 11.15. Investigative findings shall be based on facts and related analysis, which may include reasonable inferences.
- 11.16. All investigations conducted by an Investigative Officer are administrative in nature, are subordinate to, and do not remove or change the rights and obligations of Company Officials or third parties under any applicable national or international laws or under contract.

RIGHTS AND OBLIGATIONS

- 11.17. All Company Officials or third parties are obliged to report any suspected Sanctionable Practice or other suspected misconduct to the relevant Investigative Officer or the ABAC Reporting Officer/Compliance Officer. Any allegation of Integrity Violation or other suspected misconduct must be passed by the third party of the allegation to the relevant Investigative Officer Or the ABAC Reporting Officer/Compliance Officer.
- 11.18. Whistle-blowers shall not be subject to retaliation. Any retaliation will be treated as a separate act of misconduct.
- 11.19. The Company and third parties have a duty to cooperate fully in any screening or investigation when requested by an Investigative Officer to do so. Such cooperation includes, but is not limited to:
 - 11.19.1. being available to be interviewed and replying fully and truthfully to all questions asked;
 - 11.19.2. providing the Investigative Officer or such advisors as the Officer may have appointed to assist with any investigation with any items requested that are within

- the Company's or third party's control, including, but not limited to, electronic documents and data;
- 11.19.3. cooperating in any testing required by the Investigative Officer;
- 11.19.4. preserving and protecting confidentiality of all information discussed and/or secured during the investigation; and
- 11.19.5. the company or third party who is the subject of an investigation must allow it or his/her financial information to be provided directly to the Investigative Officer. Upon the Investigative Officer's request, the subject must provide written authorisation addressed to his or her bank to this effect, waiving any privacy or confidentiality rights the subject may otherwise have related to the information to be disclosed.
- 11.20. If the Company or third party is subject to an investigation, they may request to be accompanied by a third party (including legal counsel) at their own cost during interviews conducted as part of an investigation so long as such request does not delay or impede the investigation. Both subjects and witnesses may consult, at their own expense, with legal counsel so long as such consultation does not delay the conduct of the interview or compliance of the Company or third party with any obligations under this Policy, unless permitted by the Investigative Officer.
- 11.21. If the Company or third party does not comply with any obligation to cooperate, the Investigative Officer may draw an adverse inference from such refusal. In such cases, the Investigative Officer may refer the matter to the Compliance Officer and/or CRO (as the case may be) for appropriate disciplinary action. Failure to cooperate shall include not responding in a timely and complete manner to enquiries, failure to provide relevant documents or other relevant evidence that the Investigative Officer may request unless any of the exceptions set out in Section 8.7 below apply, destroying or concealing evidence or misrepresenting facts during, or otherwise inhibiting an investigation.
- 11.22. The Company or third party shall use their commercially best endeavours to include in their contracts with third parties that are financed using the Company's funds, provisions stipulating that parties involved in the investigative process shall cooperate with an investigation.
- 11.23. As part of the investigative process, the subject of an investigation shall be given an opportunity to explain his or her conduct and present information on his or her behalf.

12. THE INVESTIGATIVE PROCESS

- 12.1. All investigations should be conducted expeditiously within the constraints of available resources.
- 12.2. The Investigative Officer should examine both inculpatory and exculpatory information.
- 12.3. The Investigative Officer shall maintain and keep secure an adequate record of the information and the information collected for a minimum of six (6) years from receiving the complaint.
- 12.4. The Investigative Officer shall take appropriate measures to prevent the unauthorised disclosure of investigative information.
- 12.5. The Investigative Officer shall document its investigative findings and conclusions.
- 12.6. The Investigative Officer shall have full and unrestricted access to information and records (including e-mails) relating to the relevant Company activities. The Investigative Officer may examine any and all files, records, books, data, papers and any other materials related to a Company Official as and when deemed necessary; and take temporary possession of any material; and make copies.
- 12.7. If the Investigative Officer is required to disclose any information relating to an investigation to the Head of Investigation and Board, or an authorised third party the Investigative Officer shall require such third party to protect the confidentiality of such information and use it only for the purpose for which the Investigative Officer has disclosed the information before disclosing such information.

- 12.8. Notwithstanding any obligation under this Policy, a Company Official or third party shall not be required to disclose or provide access to any information or records (including e-mail) to an Investigative Officer if such material falls within any of the following exceptions:
- 12.8.1. information of a commercially sensitive nature and/or with respect to which the Company Official or third party owes a duty of confidentiality (the breach of which may result in penalties and/or legal action against the Company Official or third party) and where the Company Official or third party has requested consent to disclose the information but that consent has not been given and the Company Official or third party has provided the reasons for such consent being withheld; and that a confidentiality undertaking by the Investigative Officer will not enable the Company Official or third party to disclose the information without penalty and/or legal action against the Company Official or third party;
 - 12.8.2. personal information that cannot be disclosed by a Company Official or third party under applicable data protection or equivalent legislation;
 - 12.8.3. any information subject to legal privilege; or
 - 12.8.4. any information where the disclosure of such information would violate applicable law or regulations.

13. WHISTLEBLOWING POLICY & PROCEDURAL GUIDELINES

- 13.1. The Company shall provide a secured reporting system that guarantees anonymity to encourage whistleblowers to make reports in good faith.
- 13.2. The existence of this reporting system shall be communicated to all stakeholders previously identified in 1.5, and training will be provided for employees alongside monitoring and review process under 20.2 & 20.3. Contents of this training will include, but not limited to:
 - 13.2.1. Bribery as defined in this Policy
 - 13.2.2. Risks and damages that may arise from bribery
 - 13.2.3. Employee duties to comply with Anti-Bribery Policy and associated policies
 - 13.2.4. The consequences of non-compliance on employees, the Company, and other stakeholders
 - 13.2.5. Procedure for lodging a complaint, whistleblower rights and protection
- 13.3. The Investigative Officer shall accept all complaints, irrespective of their source, including complaints from anonymous or confidential sources. The Investigative Officer shall acknowledge receipt of all complaints within twenty-four (24) hours upon receipt of a complaint.
- 13.4. Each complaint will be evaluated by the Investigative Officer to determine its credibility, materiality and verifiability and whether there is a legitimate basis to warrant an investigation. The following criteria shall be used to determine whether a complaint warrants further investigation:
 - 13.4.1. relates to the Company's activities;
 - 13.4.2. credible – there is a reasonable possibility that a violation occurred;
 - 13.4.3. verifiable – practicable options exist to obtain sufficient evidence to determine the truth of the allegations on the balance of probabilities;
 - 13.4.4. material– the matter is of sufficient importance to justify the projected requirements of investigation and any remedial action; and
 - 13.4.5. other relevant considerations, e.g. whether the matter may be effectively addressed through the administrative sanctions available to the Company and the potential impact of the infraction.
- 13.5. At the conclusion of the initial evaluation, the Investigative Officer shall recommend closure of the complaint or further investigation to the Head of Investigation. Decisions to close a case at the conclusion of the initial evaluation shall be documented, setting out the reasons

- for the decision. Recommendations for further investigation shall also be set out in an Investigative Plan submitted to the Head of Investigation, which shall set out the investigative activities to be carried out. Investigative activities include the collection and analysis of documentary, video, audio, photographic and electronic information or other material, interviews of witnesses and such other investigative techniques as are required to conduct the investigation.
- 13.6. The planning and conduct of an investigation and the resources allocated to it should take into account the gravity of the allegation and the possible outcome(s).
 - 13.7. The Investigative Officer shall, wherever possible, seek corroboration of the information in its possession.
 - 13.8. Investigative activities and critical decisions shall be documented in writing and reviewed by the Head of Investigation.
 - 13.9. If at any time during an investigation, the Investigative Officer considers that it is appropriate and would be prudent, as a precautionary measure or to safeguard information, to procure the temporary exclusion of a Company Official that is the subject of an investigation from access to his or her files or office, or to recommend that he or she be suspended, with or without pay or benefits, or to recommend placement of such other limits on his or her official activities, the Investigative Officer shall refer the matter to the Head of Investigation.
 - 13.10. Interviews shall be conducted by the Investigative Officer in the presence of two (2) persons who shall be independent persons appointed by the Head of Investigation.
 - 13.11. Interviews may be conducted in the language of the person being interviewed, where appropriate, using interpreters.
 - 13.12. Under no circumstances shall a witness or a subject be paid for any information, except that reasonable expenses incurred by witnesses or other sources of information may be reimbursed.
 - 13.13. The Investigative Officer may engage external parties to assist it in its investigations.
 - 13.14. If the Investigative Officer does not find sufficient information during the investigation to substantiate the complaint, it will document such findings and notify the Head of Investigation. The Head of Investigation must approve the closing of any investigation. The standard of proof that shall be determined whether a complaint is substantiated is a preponderance of evidence sufficient to support a reasonable belief, taking into consideration all relevant factors and circumstances, that on the balance of probabilities a given party has committed a violation.
 - 13.15. If the Investigative Officer finds sufficient information to substantiate the complaint, it will document its investigative findings and refer the findings to the Head of Investigation with a recommendation as to how to proceed.
 - 13.16. Where the Investigative Officer's findings indicate that a complaint by a Company Official or third party was knowingly false, the complaint will be treated as a separate act of misconduct.
 - 13.17. Where the Investigative Officer's findings indicate that there was a failure to comply with an obligation under this Policy, the Investigative Officer may refer the matter to the Head of Investigation.
 - 13.18. Where a breach of this Policy does not amount to a breach of the laws listed in Section 2, the Investigative Officer may consider whether it is appropriate to refer the complaint to the appropriate national authorities (after taking appropriate legal advice), and the Investigative Officer shall seek the unanimous approval of the Board for such a referral. Where a breach of this Policy amounts to a breach of the laws listed in Section 2, the Investigative Officer shall notify the Head of Investigations and the Board Risk and Capital Committee of its intent to refer the complaint to the appropriate authorities and thereafter refer the complaint to the appropriate authorities.

14. SANCTIONS

- 14.1. Failure to comply with this Policy by any Company Official could attract disciplinary procedures being taken by InfraCredit in addition to any charges or prosecution levied under local legislation.
- 14.2. Company Officials who do not comply with this Policy and whose actions may constitute material breaches of this Policy must be reported to the Compliance Officer and appropriately sanctioned according to internally laid down regulations.
- 14.3. In the event that a finding of bribery, corruption or other Sanctionable Practice is reached, InfraCredit will seek prosecution of the offenders wherever possible and recovery of misappropriated funds or assets and the application of appropriate penalties wherever possible, including severing all ties with the offender.

15. TREATMENT OF POLITICALLY EXPOSED PERSONS AND MEASURES TO PREVENT AND COMBAT FRAUD, BRIBERY AND CORRUPTION WITH GOVERNMENT OR PUBLIC OFFICIALS

- 15.1. A Politically Exposed Person (PEP) includes the following:
 - 15.1.1. Senior figures in the executive, legislature, administration, military or judiciary (elected or non-elected) and other branches of government;
 - 15.1.2. Senior figures in international organisations such as intergovernmental organisations, including members of senior management such as directors, deputy directors and members of the Board or equivalent functions;
 - 15.1.3. Politicians;
 - 15.1.4. Government officials or senior executives of government owned entities;
 - 15.1.5. Heads of State;
 - 15.1.6. Senior political party officials;
 - 15.1.7. Embassy, Consular or High Commission officials;
 - 15.1.8. Members of Royal Families;
 - 15.1.9. Immediate family, partners and close associates of PEPs (immediate family means parents, siblings, spouse(s), children, grandparents, grandchildren and close relations through marriage/partnership);
 - 15.1.10. Companies, trusts, partnerships or other such entities in which any of the above have an interest directly or indirectly;
- 15.2. In addition to the close scrutiny required to be carried out above, InfraCredit must take the following steps to prior to dealing with PEPs:
 - 15.2.1. Obtain senior management approval before establishing business relationships with PEPs, where applicable;
 - 15.2.2. In-depth investigation to establish the source of funds of investors/potential investors identified as PEPs; and
 - 15.2.3. Ongoing monitoring of the business relationship.

16. MEASURES TO BE TAKEN IN DEALING WITH PUBLIC OFFICIALS

- 16.1. Company Officials, Issuers, and such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall not offer or receive Bribes, Kickbacks, Facilitation Payments, or any portion of a contract payment to or from Public Officials.
- 16.2. Company Officials, Issuers and such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall not connive with Public Officials to circumvent the law.
- 16.3. Company Officials, Issuers and such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall ensure that all

dealings with Public Officials comply with the law and are properly documented, including the issuance of properly documented official invoices and receipts.

POLITICAL CONTRIBUTIONS

- 16.4. Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees should recognize that Political Contributions can be used to obtain unfair advantages and may lead to Corruption.
- 16.5. Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall not make any direct or indirect Political Contribution without the prior written approval of the Company.
- 16.6. The Company respects the right of Company Officials and such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees to make personal Political Contributions, provided they are not made, and perceived as not made, in any way to obtain a business advantage for the Company. In particular, Company Officials and such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees must:
 - 16.6.1. not use the Company's time, assets and resources to carry out or support personal political activities;
 - 16.6.2. always make clear that views and actions are personal, and not that of the Company; and
 - 16.6.3. seek the written approval of the Board before seeking or accepting a public office.

17. CHARITABLE DONATIONS

- 17.1. Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall not use Charitable Contributions and sponsorships as subterfuge for any form of Bribery and Corruption.
- 17.2. All Charitable Contributions made by or on behalf of the Company must receive the prior written approval of the Board and thereafter must be properly documented and reported to the Board. The Board shall ensure that Charitable Contributions are publicly disclosed in the Company's annual reports.

18. GIFTS AND HOSPITALITY

- 18.1. Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall not receive, offer, solicit or arrange through third parties any Bribe, whether or not intended for his/her benefit or the benefit of a family member, friend, associate or acquaintance.
- 18.2. Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees may offer or receive gifts or benefits to the extent, in the manner and on the occasions recognized by the Company. Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees shall, before offering or receiving any gift or benefit, ensure that such gift or benefit meets the following requirements:
 - 18.2.1. it is not given, and cannot be perceived, as a Bribe;
 - 18.2.2. it complies with the law;
 - 18.2.3. it is given in the name of the Company, not in the name of an individual;
 - 18.2.4. it does not include cash or a cash equivalent (such as gift certificates or vouchers);
 - 18.2.5. it is appropriate and reasonable in light of all relevant circumstances;
 - 18.2.6. taking into account the reason for the gift, it is of an appropriate and reasonable type and value and it is given at an appropriate time;
 - 18.2.7. it is given without any expectation;

- 18.2.8. it is given openly, not secretly; and
- 18.2.9. it does not involve a Public Official.
- 18.3. The Company Officials and management shall obtain the prior written approval of the Executive Management Committee before offering or receiving any gift or benefit to or from a Public Official. In the case of Directors, approval shall be given by the Chairman of the Board, and in the case of Company Officials, approval shall be given by the Chief Executive Officer and/or the Executive Management Committee.
- 18.4. Any gift or benefit given to or received by any Director in accordance with this Section 18 shall be immediately reported to the Company and recorded by the Admin Manager, Head of Compliance and/or Chief Risk Officer. The management shall make their reports to the Board.
- 18.5. Any non-cash gift or benefit given to any staff shall not be above Two Hundred US Dollars (\$200) or Two Hundred Thousand Naira (NGN200,000), whichever is higher and must be declared to the Compliance Team and recorded in the gift register. Where such gift is above the limit (\$200 or NGN200,000), the gift will be withheld by the Compliance Team, which shall decide whether to return based on reputation risk, deliver to staff, or divide amongst personnel. The Admin Manager shall acknowledge the gift received from a third party or client in the Gift Register.
- 18.6. Any monetary honorarium (e.g. cheque, cash, transfer, etc.) given or offered to any staff must be declared to the Compliance Team and recorded in the gift register. Such an honorarium is to be retained by the Company and not handed over to the staff. This is to avoid unintended consequences, given that the honorarium represents payment for professional duties carried out on behalf of the Company.
- 18.7. All other forms of honorariums will be subject to the gift limit of NGN1,000,000 (One Million Naira).
- 18.8. The company officials (such persons and entities which receive funding either directly or indirectly from the Company or benefit from its credit guarantees) and third parties (as the case maybe) shall notify the Company before offering or receiving any gift or benefit to or from a Public Official.
- 18.9. Notwithstanding the above, no gift or benefit authorised by the Company shall exceed the sum of NGN1,000,000 (One Million Naira).
- 18.10. The Company also commits that it will not conduct transactions with or on behalf of Shell Banks.

19. NO INTERMEDIARIES

- 19.1. This Policy forbids the Company, Company Officials, Issuers and third parties which receive funding either directly or indirectly from the Company or benefit from its credit guarantees from either using an agent or making a payment to any person or entity related to a local or foreign official(s). The Policy does not permit payment to any intermediaries, including but not limited to friends, business associates or relatives of government officials, in order to circumvent this Policy. In particular, be aware that payment or favours made to any close friend or close relative of a government official involved in the Company or its affiliates, whether from the Company's funds or a Company Official's own personal funds, will be deemed an automatic violation of this Policy and may be grounds for immediate termination from the Company. For the purposes of this Policy, a "close relative" means a spouse, partner, parent, step-parent, child, step-child, sibling, step-sibling, nephew, niece, immediate cousin, aunt, uncle, grandparent, grandchild, in-law, or a parent of an in-law.

20. PERFORMANCE EVALUATION

- 20.1. The adequacy and effectiveness of this Policy is to be assessed on a continual and regular basis (in accordance with the Board approved Internal Audit Plan) through internal audits and assessment of compliance function.
- 20.2. The monitoring and review process shall be undertaken through the Board, Risk and Capital Committee and Top Management as identified in Section 7 of this Policy.
- 20.3. In monitoring, the Company shall:
 - 20.3.1. Conduct regular trainings for staff and employees on this Policy and the anti-bribery management system;
 - 20.3.2. Conduct internal audits at least annually to review the system and assess the level of compliance with the Policy and anti-bribery requirements and objectives;
 - 20.3.3. Test controls and response to compliance failures; and
 - 20.3.4. Provide a annual report to the Finance & Audit Committee and the Board for review.

INTERNAL AUDITS

- 20.4. The Company shall conduct internal audits at least annually and report to the Board's Finance & Audit Committee. The audits shall be planned, implemented and assessed in line with the Internal Audit Plan and criteria set out by the said Finance & Audit Committee.
- 20.5. The audit shall involve a review of the anti-bribery management system, procedures, and controls including any bribery or suspected bribery, violation of this Policy, weakness in or opportunities for improvement to this Policy and the Management System.
- 20.6. The audit shall also involve a review of InfraCredit's Anti-bribery Policy in compliance with ISO 37001 Standard. The implementation of the Anti-Bribery Management System shall be tested in accordance with the ISO 37001 Standard.
- 20.7. The Company shall establish, implement and maintain an Internal Audit Programme/Plan which will include the frequency, methods, responsibilities, planning requirements and reporting of the audit process.
- 20.8. The audit process shall be conducted by a select competent and impartial auditor to who will define the audit criteria and scope for each audit; ensure that the results of the audits are reported to relevant management, the anti-bribery compliance function, top management and, as appropriate, the governing body.
- 20.9. The Company shall retain documented report information as evidence of the implementation of the audit programme/plan and the audit results. These audits shall be reasonable, proportionate and risk based. Such audits shall consist of controls and systems for:
 - a) bribery or suspected bribery;
 - b) violation of the anti-bribery policy or anti-bribery management system requirements;
 - c) failure of business associates to conform to the applicable anti-bribery requirements of the organization; and
 - d) weaknesses in, or opportunities for improvement to, the anti bribery management system.
- 20.10. The Company shall ensure the objectivity and impartiality of the audit plan. The audits shall be undertaken by an independent function or personnel established or appointed for this process. The anti-bribery risk assessment may be conducted by the Compliance function. The organization shall ensure at all times that no auditor is auditing his or her own area of work.
- 20.11. The audit shall be independent and objective and may be undertaken by either an appropriate third party or independent personnel appointed for this process.

PLANNING AND IMPROVEMENTS

- 20.12. Where a violation of this Policy or weakness in the anti-bribery management system is identified or where there is non-conformity, the Company shall:
 - 20.12.1. determine the cause of the non-conformity and weakness identified;

- 20.12.2. react promptly by taking action to control and correct it as well as deal with the consequence; and
- 20.12.3. evaluate the weakness, violation or non-conformity to ensure that it does not recur or occur elsewhere.
- 20.13. The Company shall also review all improvements and corrective actions undertaken on the anti-bribery management system, determine if any changes are necessary to the system and this Policy and make such changes accordingly.
- 20.14. Where changes are required, the Company should consider the purpose of the changes and their consequence, the allocation and reallocation of responsibilities and authority and the rate, extent and timeframe for implementing the changes.

21. REPORTING REQUIREMENTS

- 21.1. In addition to such other reporting requirements as may be required of the Company, the Company shall confirm in its Annual Report and Financial Statement for each year that to the best of its knowledge and belief:
 - 21.1.1. neither it nor any other person acting on its behalf, has engaged in any activity, nor entered into any transaction, prohibited by this Policy or any of the laws in Section 2;
 - 21.1.2. after due inquiry, it is not involved with any party that is an entity or person (i) sanctioned pursuant to any United Nations Security Council resolution issued under Chapter VII of the UN Charter, (ii) on the World Bank Listing of Ineligible Firms from time to time (www.worldbank.org/debarr or any successor website or location) or (iii) convicted, indicted, or subjected to any similar criminal sanction, by any court or governmental body of competent jurisdiction, for engaging in bribery or corrupt practices or any Sanctionable Practice; and
 - 21.1.3. InfraCredit supported projects are in compliance with their obligations under this Policy.

22. AMENDMENTS

This Policy may be amended from time to time by the Compliance Officer with the consent of the Executive Management Committee.

23. COMMUNICATION

The Company's communication system will be both internal and external with respect to the anti-bribery management system. The Whistleblowing Policy of the Company shall be referenced with investigations and antibribery related matters. Such communication shall include:

- 23.1. All communication required to be given under this Antibribery & Corruption Policy and its Management System shall be in writing and may be hand-delivered or sent by courier or electronic mail.
- 23.2. Communications under this Antibribery & Corruption Policy and Management system shall be carried out from time to time and on a need basis.
- 23.3. The Company shall make communications to its Stakeholders, investors, staff, and the general public from time to time.
- 23.4. The Company shall make communications through its official website, its whistle blowing process, its Annual Report, Financial Statement for each year and such other means it deems fit to make in the appropriate circumstance.
- 23.5. The Board shall be responsible for the general communication of the Company. The Compliance Officer of the Company shall manage such communication from time to time.
- 23.6. Communication with respect to this Policy and System shall be in English Language.

24. AVAILABILITY

The Company will make the Policy and procedure publicly available, by posting it on the Company's website.

25. CHANGES TO THE POLICY

The Company reserves the right, at its absolute discretion, to change the Policy from time to time as it considers necessary. Any changes to the Policy will be timely communicated.

26. POLICY REVIEW

The Policy shall be reviewed and approved by the Board once every two (2) years to ensure its continued adequacy and relevance. Any proposed amendments shall be submitted to the Board Finance and Audit Committee for consideration and recommendation to the Board for approval.

POLICY SECTION B

ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM AND COMBATING PROLIFERATION FINANCING POLICY

1. INTRODUCTION

1.1. Policy statement

InfraCredit is built on trust and integrity as perceived by our stakeholders. An important element of trust and integrity is ensuring that InfraCredit conducts its business in accordance with the Code of Ethics and values as adopted by InfraCredit and in compliance with applicable laws, rules and regulations. InfraCredit therefore is committed to the highest levels of anti-money laundering (AML)/combating the financing of terrorism (CFT) and combating proliferation financing (CPF) compliance and requires management and all staff to adhere strictly to the provisions of this policy.

The AML/CFT/CPF ("The Policy") is designed to comply with applicable statutory and regulatory obligations as stipulated by the Money Laundering (Prevention and Prohibition) Act 2022, Terrorism (Prevention and Prohibition) Act 2022, Proceeds of Crime (Recovery and Management) Act 2022, and SEC Capital Market Operators AML/CFT/CPF Regulations 2022.

The Policy ensures that:

- The risks arising from money laundering and terrorist financing are prevented and managed;
- Relevant statutory and regulatory obligations are complied with; and the
- Reputation and integrity of InfraCredit and its employees are protected.

The Policy adopts a risk-based approach, in the identification and management of the reputational and financial risks related to money laundering, terrorist financing and proliferation financing. This Policy applies to InfraCredit, its entire staff, the Board of Directors and reflects InfraCredit's minimum requirements in respect of AML/CFT/CPF controls.

1.2. MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING – DESCRIPTION

1.2.1. Money Laundering

The act of money laundering is the process employed by criminals to disguise the illegal origin and/or illegitimate ownership of an asset which is acquired by their criminal activities. Such designated categories of offences may include forgery of money, robbery, drug, organised crime, bribery, corruption, extortion, robbery, terrorism etc.

The following acts are generally construed as acts of money laundering:

- a. Concealing, disguising, converting, transferring or removing criminal property from the territory of the crime.
- b. To enter into or become concerned personally or on behalf of another individual, in an arrangement which you know or suspect will assist the acquisition, retention, use or control of criminal property.
- c. Acquiring, using or possessing criminal property.

1.2.2. Terrorist Financing

Terrorist financing can be defined as directly or indirectly, providing or collecting funds with the intention or knowledge that they will be used in full or part to support acts of terrorism. Terrorist

financing involves the financing of terrorist acts, and of terrorists and terrorist organisations.

1.2.3. Proliferation Financing

Proliferation financing is the act of providing funds or financial services used for the manufacturing, acquisition, development, export, or transport of nuclear, chemical or biological weapons and their delivery systems, typically in violation of international sanctions or national laws. It involves moving money to enable weapons spread.

Money Laundering, terrorist financing and proliferation financing are global phenomena that compromise the security and effectiveness of financial systems, undermines economic development and damages societies. AML/CFT/CPF laws have been enacted in most countries and informed by the recommendations of the Financial Action Task Force (FATF), one of which states that countries should require financial institutions to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

To this effect, all Financial Institutions are required to deny terrorists and criminals access to the financial system and comply with all applicable AML laws and regulations.

1.3. ANTI-MONEY LAUNDERING POLICY OBJECTIVES

The purpose of this Policy is to define the minimum standards and set out required measures which must be followed to prevent InfraCredit from being used for money laundering, terrorism financing and proliferation financing activities.

The Policy applies to InfraCredit, all directors, officers and staff within InfraCredit and across all businesses and operations of InfraCredit.

In addition, this Policy will:

- Establish clear roles and responsibilities to manage money laundering, terrorist financing and proliferation financing risks.
- Communicate InfraCredit's zero tolerance policy to money laundering, terrorist financing and proliferation financing.
- Specify controls to be deployed by InfraCredit to prevent and identify money laundering, terrorist financing and proliferation financing activities in InfraCredit's operations.
- Initiate procedures to ensure that suspicious activity is reported in accordance with requirements prescribed by local laws and regulations and shared, where legally permissible and relevant, within InfraCredit.
- Serve as a reference guide for all Compliance and AML related issues.

2. ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING

2.1. AML POLICY GOVERNANCE

2.1.1. Board Oversight

The Board through the Finance and Audit Committee shall consider reports on compliance with internal policies, programs and procedures. It is also required to review and evaluate, any reports on money laundering and financial crimes produced by InfraCredit's Head of Compliance and the actions taken by senior management in relation to these reports. These reports may be flagged in the Integrity Due Diligence report produced by the Compliance Unit.

2.1.2. Board Finance and Audit Committee

The Board Finance and Audit or Credit Committee shall:

- a. Review the AML/CFT/CPF Policy and make recommendations to the Board.
- b. Monitor InfraCredit's AML/CFT/CPF performance and compliance with the Policy.
- c. Review breaches of the Policy and actions taken by senior management/executives to resolve such issues.

2.1.3. Executive Oversight

2.1.3.1. Managing Director/Chief Executive Officer

The Managing Director/Chief Executive Officer shall:

- a. Effectively manage InfraCredit's AML /CFT/CPF process across the business.
- b. Assign responsibilities to ensure the effective management of the identified money laundering, terrorist financing and proliferation financing risks.
- c. Ensure that there is a right tone at the top.
- d. Put in place appropriate policies and controls and ensure that they are effective.
- e. Ensure that the AML/CFT/CPF compliance function is adequately resourced and that there are adequate levels of delegation.
- f. Allocate any other required roles and responsibilities to appropriate staff to treat and monitor risks.
- g. Ensure organizational compliance with the Policy and that non-compliance is sanctioned.

2.1.3.2. Senior Executives

- a. Ensure that the requirements of the Policy are incorporated into Divisional processes.
- b. Be accountable for delivering the outcome of AML/CFT/CPF processes and procedures in their particular area of responsibility.
- c. Support the Head of Compliance in the execution of the responsibilities of his/her positions.

2.1.3.3. AML/CFT/CPF Compliance

The Head of Compliance shall be given overall responsibility within the organisation for the establishment and maintenance of effective AML/CFT/CPF systems and controls consistent with the requirements of the relevant AML/CFT/CPF laws and regulations.

The Head of Compliance shall take on the role of the Money Laundering Reporting Officer (MLRO) and be the contact person between InfraCredit and regulators.

The Head of Compliance shall have the relevant competence, authority and independence within the organisation and have access to resources and information sufficient to enable him/her carry out stipulated responsibilities and shall deal with all disclosures confidentially and make decisions on the reporting of suspicious activity. The Head of Compliance shall report directly to the Board on all AML related issues.

The Head of Compliance must be familiar and ensure compliance with all legislations and regulations to combat money Laundering, terrorism financing and proliferation financing as stipulated by the Nigerian Government.

2.1.3.4. General Responsibilities

The roles and responsibilities of the Money Laundering Reporting Officer (MLRO) include:

- a. Develop and implement the AML/CFT/CPF programme and present same to the Board for

- approval;
- b. Report suspicious persons/entities and activities to the relevant authorities in the appropriate manner, where applicable;
- c. Develop and review, at least once in two years, AML/CFT/CPF processes and procedures and provide enhancement recommendations, as appropriate, to the Finance and Audit Committee;
- d. Monitor and review existing and new sanctions as introduced and amended and determine how they affect InfraCredit;
- e. Review, identify and update potential risk areas in the identification of money laundering and terrorist financing.
- f. Review and update procedures/frameworks set out to fight against/mitigate the threats posed by money launderers and terrorism financiers;
- g. Ensure the internal audit function of InfraCredit regularly conducts a test as to the adequacy, completeness and effectiveness of the AML/CFT/CPF compliance programme;
- h. Provide a heightened awareness of key AML/CFT/CPF issues and techniques; develop and administer comprehensive training programme for all incoming relevant staff on AML/CFT/CPF. (See Appendix 1 for Elements of an Employee Training Programme);
- i. Serve as a liaison officer between InfraCredit and relevant regulatory authorities and also as a contact person for all employees on money laundering/terrorist financing/proliferation financing and corruption related issues;
- j. Prepare reports on Know Your Customer (KYC) and Integrity Due Diligence to be considered by the New Business and Credit Committee.

2.2. AML/CFT/CPF POLICY REQUIREMENTS

2.2.1. Controls

2.2.1.1. Risk Identification

InfraCredit will subject all potential third-party relationships to a risk assessment process and will carry out necessary due diligence as required.

InfraCredit will adopt a risk-based approach in mitigating its AML/CFT/CPF associated risks. InfraCredit's business relationship is expected to be predominantly with the following categories of third parties:

- a. Investors aiming to provide InfraCredit with funds.
- b. Issuers seeking to obtain guarantees from InfraCredit.
- c. Other third parties such as vendors, suppliers and service providers.
- d. Third parties will be categorized into risk buckets: high, medium and low. The risk rating of third party will determine level of due diligence that they are subject to. Factors to be considered in assessing the risk rating of a third party include:
 Ownership of the third party: The nationality and the risk rating of the promoters, board members and shareholders of the third party.
 Geographical factors: The level of compliance in the country of domicile of the third party with FATF recommendations.
 Nature of business activity that a third party is engaged in.

2.2.1.2. Due Diligence on Third Parties

The InfraCredit team interfacing with a third-party will carry out due diligence on the third-party subject to reviews by the Head of Compliance. Due diligence will be carried out when:

- a. A new business relationship is established.
- b. There is a substantial change in third-party documentation.

- c. InfraCredit lacks sufficient information about an existing or prospective third-party.
- d. InfraCredit suspects a third-party is involved in money laundering, terrorist financing or proliferation financing.
- e. InfraCredit doubts the adequacy or integrity of previously obtained third-party due diligence data.

Due diligence procedures include but not limited to the following:

- i. Identifying the third-party (whether a natural, legal person or another type of legal arrangement) using regulatory identification documents like driver's license, international passport or incorporation documents. Refer to Appendix A2.
- ii. Gathering and verifying information on a third party to understand fully the nature of its operations and sources of funds.
- iii. Obtaining, recording and updating sufficient evidence for identity of private companies owned by a third party and verifying the addresses of majority shareholders and principal controllers of the company's assets. Records obtained should include proof of identity such as certificate of incorporation and other valid official documents showing proof of company existence.
- iv. Taking reasonable measures to verify the identity of the ultimate beneficial owner of the third party.
- v. Putting in place appropriate risk management systems to determine whether a third party or the beneficial owner is a Politically Exposed Person.
- vi. Monitoring all third parties and their activities against sanctions lists such as OFAC SDN list, UN, EU, UK and Nigeria Sanction lists.
- vii. Ensuring non-resident investor institutions' AML/CFT/CPF controls are in compliance with FATF standards.
- viii. Scrutinising all non-face-to-face business relationships.

Enhanced due diligence shall be carried out on high-risk third parties. The following shall be considered as high-risk:

- a. Politically Exposed Persons.
- b. Parties from countries that do not or insufficiently comply with FATF recommendations.
- c. High net worth individuals (HNWIs).
- d. Companies with complex ownership structures.

The above list is not exhaustive, and the Head of Compliance may classify third parties as high-risk based on information available on the entity or regulatory updates. Enhanced Due Diligence shall be carried out on high-risk customers/third parties frequently or as the need arises based on changes in their risk profile. This shall include a thorough risk assessment, ongoing transaction monitoring and periodic KYC refreshes.

2.3. RISK MITIGATION/CONTROLS

2.3.1. Politically Exposed Persons (PEP)

Whilst there is no internationally agreed legal definition of a Politically Exposed Person (PEP), they include the following:

- a. Senior figures in the executive, legislature, administration, military or judiciary (elected or non-elected) and other branches of government
- b. Senior figures in international organisations such as multinational companies and intergovernmental organisations, including members of senior management such as directors, deputy directors and members of the Board or equivalent functions
- c. Politicians
- d. Government officials or senior executives of government owned entities

- e. Heads of State
- f. Senior political party officials
- g. Embassy officials
- h. Members of Royal Families

Immediate family, partners and close associates will by implication be closely connected to the activities of the PEP and are therefore included in the categorization. Immediate family will include parents, siblings, spouse(s), children, grandparents, grandchildren and close relations through marriage/partnership.

PEPs also includes any companies, trusts, partnerships or other such entities in which any of the above have an interest directly or indirectly.

No definition is or can be exhaustive as to who should or should not be treated as PEP in a given country. Local knowledge will provide the critical information upon which a decision can be based.

PEPs are regarded as high-risk because of their ability to exercise undue influence over others and/or abuse their position of power and influence.

PEPs must be viewed from a risk/reward perspective due to the potential damage, both reputational and actual, that they could inflict upon InfraCredit.

In addition to assessing the investor/potential investor (as covered in Section 2.1.2), InfraCredit must assess the investor/potential investor's Board of Directors and, in the event that any member of its Board of Directors is flagged as a PEP, the following must be carried out:

- Obtaining of senior management approval before establishing business relationships with such PEPs.
- In-depth investigation to establish the source of funds of investors/potential investors identified as PEPs.
- Ongoing monitoring of the business relationship.

2.3.2. Prohibited Relationships

InfraCredit will not engage any form of business relationship with:

- a. Third parties whose funds/promoters are linked to money laundering or corruption and other illegal activities.
- b. Anonymous individuals or corporate bodies
- c. Shell companies
- d. Unlicensed banks
- e. Unregulated Money Service Bureau
- f. High-risk foreign banks.

2.3.3. Contractual Controls

InfraCredit will ensure that contracts entered into with third parties contain anti-money laundering clauses. An example is the following terms:

- a. That the issuer will not directly and indirectly participate in or allow its business processes to be used for money laundering, terrorist financing or proliferation financing.
- b. That if the issuer becomes aware that it is exposed or has been exposed to money laundering or terrorist financing, it will immediately inform InfraCredit of such developments.
- c. That InfraCredit retains the right to audit the issuer's books and operations InfraCredit it suspects that the issuer is participating in or is being used as a vehicle for money laundering

or terrorist financing.

3. REPORTING

3.1. INTERNAL REPORTING

Officers in all units or departments of the institution should be aware that they could be potentially exposed to money laundering, terrorist financing or proliferation financing. This may be either when conducting due diligence or in the normal course of business with the third party. It is important that all officers are aware of their responsibility to report any suspicions of money laundering activity. All officers are responsible to act promptly and report any suspicions to the Head of Compliance to prevent any breach of legislation which can lead to penalties and/or criminal prosecution.

Upon receipt of the report, the Head of Compliance may contact the staff who made the report to discuss the content of the report in detail before taking appropriate actions.

No further steps in any transaction relating to the suspected money laundering should be made without authorisation from the Head of Compliance.

No disclosure should be made to the third party or others that would indicate suspicions of money laundering. Any officer making a report should not disclose such to the third party or others as that may result in tipping off.

Where the Head of Compliance is involved in a report or a violation, such reports should be forwarded directly to the Chief Executive Officer.

All members of staff of InfraCredit are prohibited from:

- a. Assisting in money laundering, terrorist financing or proliferation financing activities.
- b. Tipping off suspected individuals upon knowing or suspecting that an investigation into money laundering is being, or about to be conducted, or a disclosure has been made to the Head of Compliance or regulators.
- c. Failing to report all suspicions of money laundering, terrorist financing or proliferation financing.

All staff members of InfraCredit are personally liable for failing to report any suspicions to the proper channel within the organisation. InfraCredit requires all staff members to always render full co-operation with the regulators and law enforcement agents when the need arises and assures such staff member(s) of confidentiality and protection from victimization.

3.2. REGULATORY REPORTING

InfraCredit shall file the following returns with the Securities and Exchange Commission (SEC):

- a. **Quarterly Returns:** within thirty (30) days after the end of each quarter, providing an overview of its financial and non-financial performance.
- b. **Annual Returns:** within three (3) months after the end of the accounting year, presenting a comprehensive financial statement and a review of its operations.
- c. **Quarterly Returns on Utilization of Issues Proceeds:** within three (3) months after the clearance of allotment (where applicable), detailing the allocation and usage of funds raised through public offerings.
- d. **Quarterly AML/CFT Returns:** within thirty (30) days after end of each quarter, providing information on its anti-money laundering and combating the financing of

terrorism (AML/CFT) policies and procedures.

- e. **Annual AML/CFT Returns:** Not later than December 31st of each year, providing information on its anti-money laundering and combating the financing of terrorism (AML/CFT) policies and procedures.

InfraCredit's policy to keep its relationships confidential shall in no way inhibit the cooperation of its employees with relevant AML/CFT/CPF regulatory authorities under this policy.

Therefore, in responding to authorised enquiries from relevant regulatory and government institutions, InfraCredit will comply with the steps below:

- Conduct an immediate search of InfraCredit's records to determine if it maintains or has in the past maintained any records/account for or has engaged in any transaction with or on behalf of the individual, entity or organisation for which such request is made.
- Promptly report the outcome of such research to the concerned relevant institution.
- Ensure the security and confidentiality of such request.

a. SANCTIONS AND PENALTIES FOR NON-COMPLIANCE WITH AML/CFT/CPF REGULATIONS

Failure to comply with AML/CFT/CPF responsibilities and regulations by any staff of InfraCredit could attract disciplinary procedures being taken by InfraCredit in addition to any penalties imposed under regulations.

Employees who do not comply with this policy and whose actions may constitute material breaches of this policy must be reported to the Head of Compliance and appropriately sanctioned according to internally laid down disciplinary procedures.

Failure to comply with **SEC AML/CFT/CPF Regulations** may attract **administrative sanctions** (including penalties, suspension of registration) and other applicable penalties under MLPPA/TPPA. InfraCredit will maintain evidence of compliance and cooperate fully with SEC and other authorities.

b. MAINTENANCE OF RECORDS

i. Records on Investors and Issuers

InfraCredit must preserve all necessary records of investors, issuers and third parties for a minimum of five (5) years following the completion of all business relationships. This requirement includes all due diligence documents, details of transactions and all other necessary documents relating to business transactions between InfraCredit and Investors/Issuers. Records must be easily accessible to the Head of Compliance and regulators on a timely basis.

A breach of this requirement may cause InfraCredit to be liable to sanctions in accordance with the provisions of the MLPA 2022 (as amended), and other laws and regulations related to money laundering and terrorism. The five-year period is in accordance with the IT Policy of InfraCredit.

ii. Other Records

All records of filings with regulators must be preserved for a minimum of five (5) years after such filings. InfraCredit must provide these records to regulators whenever they make a demand in writing.

c. POLICY REVIEW

InfraCredit has designed its AML/CFT/CPF program to align with global leading practices and shall be reviewed and approved by the Board once every two (2) years to ensure its continued adequacy and relevance. Any proposed amendments shall be submitted to the Board Finance and Audit Committee for consideration and recommendation to the Board for approval.

A APPENDICES

A.1 ELEMENTS OF AN EMPLOYEE TRAINING PROGRAMME

The employee training programme is to be developed under the guidance of the Head of Compliance in collaboration with the Senior Management.

The basic elements of the Training programme include:

- AML regulations and offences
- The nature of money laundering
- Money laundering red flags
- Reporting requirements
- Customer due diligence
- Risk-based approach to AML/CFT/CPF
- Record-keeping and retention policy

A.2 INFORMATION TO ESTABLISH IDENTITY

The following shall form minimum information requirement to be obtained from all Investors and Issuers with whom InfraCredit shall conduct business with. Compliance shall develop a checklist of information.

In considering the customer identification guidance for the different types of institutions, particular attention should be given to the beneficial owners of the institutions and different levels of risk involved.

At the minimum, the following information should be obtained:

- Name of institution;
- Principal place of institution's business operations;
- Brief Corporate Profile with details of Directors and Executive Management;
- Details of Significant Shareholders;
- Contact telephone and fax numbers;
- Some form of official identification number, if available;
- The original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association; CAC Form 2 and CAC Form 7
- The resolution of the Board of Directors to enter into a business relationship with InfraCredit and identification of those who have authority to represent the company in this regard;
- Nature and purpose of business and its legitimacy.

InfraCredit will verify this information by at least one of the following methods:

- Reviewing a copy of the latest report and accounts of established corporate entities;
- Conducting an enquiry by a business information service or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated;
- Utilising an independent information verification process, such as accessing public and private databases;
- Obtaining prior bank references (where necessary);
- Visiting the corporate entity; and

- Contacting the corporate entity by telephone, mail or e-mail.

InfraCredit will also conduct background checks on the promoters and executive management of investors and issuers using publicly available information. Where there is a need to conduct enhanced due diligence, enhanced background checks should be done using information from government institutions e.g. CAC and SEC.

A.3 DEFINITION OF TERMS

Terms	Definition
Beneficial Owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Business Relationship	'Business relationship' is any arrangement between the financial institution and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.
Designated Categories of Offences	Designated categories of offences means: ▪ participation in an organised criminal group and racketeering; ▪ terrorism, including terrorist financing; ▪ trafficking in human beings and migrant smuggling; ▪ sexual exploitation, including sexual exploitation of children; ▪ illicit trafficking in narcotic drugs and psychotropic substances; ▪ illicit arms trafficking; ▪ illicit trafficking in stolen and other goods; ▪ corruption and bribery; ▪ fraud; ▪ counterfeiting currency; ▪ counterfeiting and piracy of products; ▪ environmental crime; ▪ murder, grievous bodily injury; ▪ kidnapping, illegal restraint and hostage-taking; ▪ robbery or theft; ▪ smuggling; ▪ extortion; ▪ forgery; ▪ piracy; and ▪ insider trading and market manipulation
Financial Institutions	Financial institutions means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: ▪ Acceptance of deposits and other repayable funds from the public. ▪ Lending. ▪ Financial leasing.

	▪ The transfer of money or value. ▪ Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). ▪ Financial guarantees and commitments. ▪ Trading in: ✓ money market instruments (cheques, bills, CDs, derivatives etc.); ✓ foreign exchange; ✓ exchange, interest rate and index instruments; ✓ transferable securities; ✓ commodity futures trading. 1. Participation in securities issues and the provision of financial services related to such issues. 2. Individual and collective portfolio management. 3. Safekeeping and administration of cash or liquid securities on behalf of other persons. 4. Otherwise investing, administering or managing funds or money on behalf of other persons. 5. Underwriting and placement of life insurance and other investment related insurance. 6. Money and currency changing. The list is not exhaustive but subject to the definition contained in BOFIA 1991 (as amended).
Property	Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Risk	All references to risk in this Manual refer to the risk of money laundering and/or terrorist financing.
Shell Bank	Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
Terrorist	It refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist Act	A terrorist act includes but are not limited to: ▪ An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of

	Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist Financing Offence	A terrorist financing (FT) offence refers not only to the primary offence or offences, but also to ancillary offences.
Terrorist Organisation	Refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Counter-Proliferation Financing (CPF)/PF	Financing of proliferation of weapons of mass destruction; includes evasion of PF-targeted financial sanctions ; subject to UNSCRs and Nigeria's TFS regulations.
Targeted Financial Sanctions (TFS)	Asset-freezing and prohibitions mandated by UNSCRs/Nigerian law relating to TF and PF; immediate implementation and reporting to SEC/NFIU.
Beneficial Owner (SEC context)	Natural person(s) ultimately owning/controlling the customer (including senior managing official where necessary); 5% threshold applies for higher-risk private/unquoted scenarios in identification measures.
FATF Recommendations	The FATF Recommendations refers to the 40 Recommendations and to the 9 Special Recommendations by the Financial Action Ts on Terrorist Financing.
Those Who Finance Terrorism	Those who finance terrorism refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.