1 2 3 FINANCE CORPORATION

MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION PROGRAM (MTPP)

2024 VERSION

PART 1 – OVERVIEW

I. Introduction

The Anti-Money Laundering Council, comprised of the Bangko Sentral ng Pilipinas, Security and Exchange Commission, and Insurance Commission provides rules and regulations to covered institutions relative to the implementation of R.A. 9160 also known as The Anti-Money Laundering Act (AMLA) of 2001, as amended by R.A. 9194, R.A. 10167, R.A. 10365 and R.A. 10927, and R.A. 10168 also known as The Terrorism Financing Prevention and Suppression Act (TFPSA) of 2012.

II. Company Profile and Organizational Structure

1 2 3 FINANCE CORPORATION ("Corporation") is a domestic stock corporation founded in 18 January 2018 with the primary purpose to extend credit facilities to consumers and industrial, commercial, or agricultural enterprises whether by granting direct loans or by discounting or factoring commercial papers or accounts receivables for profit, buying and selling contracts, leases chattel mortgages, and other pieces of evidence of indebtedness arising out of one or more of the steps in the distribution and sale of commodities. The registered principal office address of the Company is located at 1600 Pedro Gil St. Cor. J. Bocobo St., Malate, Manila 1004.

The Corporation's organizational hierarchy includes Processing, Assessment, Collection, Accounting, Compliance, Human Resources, Legal, Information Technology, Customer Service, and Marketing Departments. Senior management, led by the President of the Corporation, oversees the strategic direction. While the Board of Directors ensures governance and compliance and the Corporation's compliance officers diligently monitor AML/CTF practices.

III. Legal Framework

This MTPP considers the Updated AMLA and TFPSA Rules and Regulations under BSP Circular 1022 dated November 26, 2018, and the Security and Exchange Commission Certification Examination Anti-Money Laundering (AML) Module issued on March 28, 2019, AML risk and AML risk management, internal policies and procedures, and industry sound practices.

IV. Policy Statement

This MTPP is designed to ensure that the Corporation shall comply with the AML and Countering of Terrorist Financing (CTF) requirements and obligations set out in Philippine legislation, rules, regulations, government regulatory bodies and agencies' guidance, global best practices; and that adequate systems and controls are in place to mitigate the AML risks and that the Corporation is not used to facilitate financial crime.

V. Policy Objectives

The Corporation aims to reduce our exposure to AML/CTF risks by implementing robust controls and due diligence processes. Our MTPP ensures strict adherence to relevant laws, regulations, and guidelines. The Corporation promptly identify suspicious activities and report them to relevant authorities. The Corporation will educate its employees about AML/CTF policies and procedures for effective implementation.

By aligning with these objectives, the Corporation contribute to a safer financial environment.

VI. Policy Scope

This MTPP applies to all services offered by the Corporation. All branches and affiliates fall under the MTPP's purview to ensure comprehensive AML/CTF compliance.

VII. Definition of Terms

Agent is any individual or entity authorized to act on behalf of a customer in any capacity, such as executing transactions, managing accounts, or making decisions. Examples include legal representatives, intermediaries, and authorized signatories.

Beneficial owner is an individual who owns or controls 25% or more of a legal entity, either directly or indirectly. This includes individuals with significant influence over the entity's operations or decision-making processes.

Customer/ Client refers to any person or entity who keeps an account or otherwise transacts business with a covered person.

Customer Due Diligence refers to the procedure of identifying and verifying the true identity, of customers, and their agents and beneficial owners, including understanding and monitoring of their transactions and activities.

Enhanced Due Diligence refers to the enhanced level of scrutiny intended to provide a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, to mitigate risks presented.

Financing of terrorism is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects, or uses property or funds or makes available property, funds financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (1) to carry out or facilitate the commission of any terrorist act; (2) by a terrorist organization, association or group; or (3) by an individual terrorist.

Monetary instrument refers to coins or currency of legal tender of the Philippines, or any other country; drafts, checks, and notes; securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts or deposit substitute instruments, trading orders, transaction tickets and confirmations of sale or investments and money market instruments; and other similar instruments where title thereto

passes to another by endorsement, assignment or delivery.

Money Laundering Offense is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity: (a) transacts said monetary instrument or property; (b) converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property; (c) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights to said monetary instrument or property; (d) attempts or conspires to commit money laundering offenses referred to in paragraphs (a), (b) or (c); (e) aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (a), (b) or (c) above; and (f) performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraphs (a), (b) or (c) above. Money laundering is also committed by any covered person who fails to do so knowing that a covered or suspicious transaction is required under this Act to be reported to the Anti-Money Laundering Council (AMLC).

Politically Exposed Persons (PEPs) are individuals who hold or have held prominent public positions, such as heads of state, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, and important political party officials.

Proceeds refer to an amount derived or realized from an unlawful activity.

Proliferation financing refers to when a person makes available an asset; provides a financial service; or conducts a financial transaction; and the person knows that, or is reckless as to whether, the asset, financial service, or financial transaction is intended to, in whole or in part, facilitate proliferation of weapons of mass destruction in relation to UN Security Council Resolution Numbers 1718 of 2006 and 2231 of 2015. (As amended by Sec. 2 of Republic Act No. 11521)

Risk refers to the risk of loss arising from ML/TF activities.

Risk Assessment refers to the process by which countries, competent authorities, and covered persons identify, assess, and

understand the ML/TF risks to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. This includes prioritization and efficient allocation of resources by the relevant key players and stakeholders in applying AML/CTF measures in their operations in a way that ensures that they are commensurate with the risks involved.

Supervising Authority refers to the appropriate supervisory or regulatory agency, department, or office supervising or regulating the covered institutions enumerated in Section 3(a).

'Targeted financial sanctions refer to both asset freezing and prohibition to prevent funds or utter assets from being made available, directly or indirectly, for the benefit of any individual, natural or legal persons or entity designated pursuant to Revant United Nations Security Council resolutions and its designation processes.

Tipping-off refers to the act of disclosing to a customer or third party that they are subject to an investigation or that a suspicious activity report (SAR) has been filed against them. Examples include informing a customer that their transaction is being monitored or that their activities have been reported to authorities.

PART 2 – GOVERNANCE AND OVERSIGHT

I. Institutional Risk Assessment and Management

The risk assessment and management process is a critical component of the Corporation's MTPP, enabling us to identify vulnerabilities and implement effective measures to mitigate money laundering and terrorism financing risks.

The Corporation systematically identifies risk factors across operations, including customer profiles, service offerings, and geographic exposure. The risk assessment methodology involves collecting and analyzing data from various sources, using statistical and trend analysis to evaluate potential risks.

To address identified risks, the Corporation implements a range of mitigation measures, including enhanced due diligence procedures, transaction monitoring systems, and customer screening protocols. For high-risk customers, we apply enhanced due diligence measures. The Corporation's transaction monitoring system detects suspicious activities promptly.

By assessing and managing risks effectively, the Corporation's measures are designed to detect and prevent money laundering and terrorism financing activities and contribute to a resilient AML/CTF framework.

II. Corporate Governance

The Corporation's Board of Directors and AML/CTF Compliance Officers play a pivotal role in the MTPP.

The Board of Directors actively participates in AML/CTF governance. They set policies, oversee risk management, and ensure compliance with regulatory requirements. Whereas, the AML/CTF Compliance Officers translate policies into action. They monitor daily AML/CTF activities, conduct regular risk assessments, and ensure adherence to policies and procedures. It acts as a central point for all AML/CTF-related matters within the organization.

III. Compliance Management

The Corporation shall appoint a senior officer as the Compliance Officer.
A Compliance Officer shall be:

(a) A senior officer with relevant qualifications and experience to enable him/her to respond sufficiently well to inquiries relating to the relevant person and the conduct of its business;
(b) Responsible for establishing and maintaining a manual of compliance procedures with the business of the Corporation.
(c) Responsible for ensuring compliance by the staff of the Corporation with the provisions of the Act, its Implementing Rules and Regulations, and the MTPP;
(d) Responsible for disseminating all memorandum circulars, resolutions, instructions, and policies issued by the AML Council and the Security and Exchange Commission (SEC) in all matters relating to the prevention of money laundering;
(e) The liaison between the Corporation and the AML Council in matters relating to compliance with the provisions of the Act and its Implementing Rules and Regulations; and
(f) Responsible for the preparation and submission to the AML Council written reports on the Corporation's compliance with the provisions of the Act and its Implementing Rules and Regulations, in such form as the AML Council may determine, and within such period as the SEC may allow in accordance with the AMLA, as amended.

Notwithstanding the duties of the Compliance Officer, the ultimate responsibility for proper supervision, reporting, and compliance pursuant to the AMLA, as amended, its Revised Implementing Rules and Regulations shall rest with the Corporation's Board of Directors.

IV. Internal Controls and Audit

The Corporation is required to establish and implement internal control procedures aimed at preventing and impeding money laundering. These procedures shall ensure that intermediaries and their employees are aware of the provisions of the law, its implementing rules and regulations, as well as all reportorial and compliance controls and procedures established by the AML Council and the Corporation.

The Corporation's policies and procedures should cover:

- Communications of firm policies relating to money laundering, including timely disclosure of information and internal audits to ensure compliance with policies, procedures, and controls;
- Account opening and customer identification requirements;
- Maintenance of records;
- Compliance with the AMLA, as amended, its Revised Implementing Rules and Regulations, and all Circulars issued by the Commission and the AML Council;
- Cooperation with the SEC and other relevant authorities.

The Corporation shall establish written internal reporting procedures which shall:

a. Enable all directors, officers, employees, and key staff to know to whom they should report any knowledge or suspicion of money laundering activity;
b. Ensure a clear reporting chain directing suspicions to the Compliance Officer in accordance with Corporation's Reporting Procedures.
c. Require the Compliance Officer to consider any report in light of all relevant information to determine whether it indicates knowledge or suspicion of money laundering;
d. Ensure the Compliance Officer has reasonable access to any other information that may assist in determining whether a suspicious transaction report is to be filed;
e. Require that upon determination of the suspicious nature of the report, the information contained therein is disclosed promptly to the Council.

V. Hiring Policies and Procedures

It is the practice of the Corporation to recruit only the best-qualified applicants available in the labor market and to employ fair and consistent policies in the process of recruitment, selection, and placement.

The Corporation follows the hiring process to ensure that all key aspects of the recruitment have been addressed.

Temporary, emergency, and other abridged-process hires will not require all steps to be completed.

Hiring Procedure is as follows:

1. Identify Vacancy and Evaluate Need;
2. Develop Position Description;
3. Post and Advertised Position;
4. Review Applicants and Develop Short List;
5. Series Interview;
6. Select Hire and check character references; and
7. Job Offer Signing.

Before any employee is hired on a probationary or direct regularization basis, the following are required:

a. SSS number;
b. PAG-IBIG number;
c. PhilHealth number;
d. Tax Identification Number/ Form 2316 ITR;
e. NBI Clearance;
f. Clearance from last employer (if applicable);
g. Withholding Tax Exemption Certificate (if applicable);
h. ID pictures (1x1) - 2 copies;
i. Birth Certificate (PSA);
j. Marriage Contract (if Married Employee);
k. Transcript of Record; and
l. Medical Clearance/Certificate (CBC/URINE/STOOL/XRAY/).

The final approval of hiring any employee will rest with the President and CEO, although the President and CEO may from time to time give that authority to another senior manager.

PART 3 – POLICIES AND PROCEDURES

I. Customer Acceptance and Due Diligence:

1. *Customer Identification / Know-Your-Customer*

The Corporation shall obtain from all individual applicants the following information:

a. Name and/or names used;
b. Present address;
c. Permanent address;
d. Mailing address;
e. Date and place of birth;
f. Nationality;
g. Nature of work, name of employer, or nature of self-employment or business;
h. Tax identification numbers, Social Security numbers or Government Service and Insurance System numbers;
i. Specimen signature; and
j. Sources of funds.

The Corporation shall request individual applicants who present only photocopies of identifications and other documents to produce the original documents for verification purposes.

2. *Customer Risk Profiling/Assessment*

The Corporation shall comply with the following guidelines for establishing the true and full identity of the clients:

a. Reduced Due Diligence for Low-Risk Clients

The Corporation shall ensure that customers, upon presentation of acceptable identification cards or other reliable and independent source documents, are eligible to avail themselves of the services provided by the corporation.

b. Average Due Diligence for Normal Risk Clients

The Corporation shall collect all minimum required information at the time of loan application and verify this information with valid identification documents from individual clients before establishing any relationship.

c. Enhanced Due Diligence for High-Risk Clients.

The Corporation, in addition to the minimum Know-Your-Customer identification requirements, shall do the following as enhanced due diligence:

c.1. Obtain additional information beyond the minimum required for average due diligence, including, to wit:

i. Supporting information on the intended nature of the relationship/source of funds/source of wealth;

ii. Reasons for the intended or performed transactions;

iii. List of banks where the individual has maintained or is maintaining an account; and

v. Other relevant information available through the public databases or the internet.

c.2. Conduct validation procedures on any or all of the information provided.

c.3. Conduct enhanced ongoing monitoring of the business relationship.

c.4. Where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, the Corporation shall deny relationship with the client/borrower without prejudice to the reporting of a suspicious transaction to the AMLC when deemed necessary.

3. *Customer Verification*

The Corporation shall verify customers by requiring specific documentation to authenticate the identity and credibility of the customers.

For primary identification, customers must provide one of the following: a passport, a Seaman's Book, or a government-issued identification.

To verify proof of employment, customers need to submit either an employment contract, a Certificate of Employment, or a visa.

For proof of address, acceptable documents include a utility bill or a barangay clearance. These documents help ensure the customer's identity and their stable employment status, crucial for the financing company's due diligence process. Face-to-face contact with clients is mandatory for processing transactions. Without such, no transaction shall be processed.

4. *Identification and Verification of Agents*

The Corporation understands who is acting on behalf of our customers and can mitigate any associated risks.

To identify an agent, the Corporation collect the following information:

- Full name
- Date of birth
- Contact details (address, phone number, email)
- Identification document number and type (e.g., passport, driver's license)
- Nature of their relationship with the customer and the extent of their authority
- Government-issued identification documents, such as a passport or national ID card, to verify their identity.

The following steps are taken to verify the information provided by agents:

- Cross-reference the agent's details with official government and financial databases.
- Validate the authenticity of identification documents using verification tools or services.
- Conduct background checks to ensure the agent has no history of financial crime or other red flags.
- In certain cases, third-party verification services may be

utilized to confirm the agent's information and background.

5. *Beneficial Ownership Verification*

To identify beneficial owners, the Corporation collects the following information:

- Full name;
- Date of birth;
- Nationality;
- Residential address; and
- Percentage of ownership or control.

Beneficial owners must provide documentation such as:

- Ownership structure charts;
- Shareholder registers;
- Legal agreements and contracts; and
- Government-issued identification documents (e.g., passports, national IDs)

Verification involves cross-referencing details with official registries and financial databases, validating ownership documents, conducting background checks for financial crimes, and using third-party services when necessary for in-depth background checks.

The Corporation assesses the risk of beneficial ownership based on business type, jurisdiction, and transaction volume. High-risk beneficial owners undergo enhanced due diligence to validate their identities and assess potential risks.

6. *Determination of the Purpose of Relationship*

The Corporation engages in discussions with customers to understand their intended business activities, assessing the legitimacy and alignment with our risk appetite and compliance requirements.

The Corporation review relevant documents such as business plans, contracts, and transaction details to ensure transparency regarding the purpose of the relationship.

The identified purpose informs our risk assessment: higher-risk activities, such as complex transactions and cross-border dealings, trigger enhanced due diligence, while lower-risk activities, like routine banking services, follow standard due diligence procedures.

7. *Ongoing Monitoring of Customer's Information and Accounts / Transactions*

The Corporation updates customer identification every three (3) years in line with BSP Circular 950 Series of 2017, ensuring compliance with ongoing monitoring requirements.

The Corporation applies enhanced due diligence if it encounters information during customer account or transaction monitoring that raises doubts about the accuracy of provided information or documents, justifies reclassification of the customer from low or normal risk to high risk based on internal criteria and knowledge that a customer was or is engaged or engaging in any unlawful activity as herein defined.

In cases where additional information cannot be obtained, or provided information or documents are false or unsatisfactory, the Company immediately closes the account and refrains from further business with the customer. This action is taken without prejudice to the reporting of suspicious transactions to the AMLC when circumstances warrant.

II. Preventive Measures for Specific Transactions and Activities

The Corporation implements preventive measures for high-risk transactions and unusual or suspicious activities to mitigate the risk of money laundering and terrorism financing.

High-risk transactions, such as large cash deposits or withdrawals, dealings with customers from high-risk countries, and transactions involving politically exposed persons, are subject to increased scrutiny and monitoring.

Unusual or suspicious activities are identified based on criteria like transaction size, frequency, and deviation from the customer's normal behavior. Examples include rapid fund movements without clear purpose, transactions inconsistent with the customer's known activities, and structuring transactions to avoid reporting thresholds.

Enhanced due diligence measures involve obtaining additional information about the customer and the transaction, verifying the source of funds, and conducting more frequent and detailed transaction monitoring.

Detailed records of all high-risk and suspicious transactions are maintained, including information about the customer, the nature and purpose of the transaction, and any supporting documentation.

III. Politically Exposed Persons

Politically Exposed Persons (PEPs) are considered at higher risk for potential involvement in corruption and other illicit activities. The Corporation complies with regulatory requirements to identify, assess, and manage the risks associated with PEPs.

The Corporation assesses the risk level of PEP-related transactions based on factors such as their current position, jurisdiction, transaction volume, immediate family members, and close associates.

To identify PEPs, the Corporation uses various sources, including government and regulatory lists of PEPs, commercial databases that provide PEP screening services, and publicly available information from reputable sources, such as news media and official websites.

IV. Transaction reporting

1. *Covered transactions*

The mandatory Covered Transaction Report ("CTR") shall be filed before the Anti-Money Laundering Council for transactions in cash or other equivalent monetary instruments involving a total amount in excess of the threshold of P500,000 within one(1) banking day as provided under Section 3 (b) of Republic Act 9160, as amended.

2. *Suspicious transactions*

The Corporation shall file a Suspicious Transaction Report (STR) before the Anti-Money Laundering Council, regardless of the amount of the transaction where any of the following circumstances exists:

1. There is no underlying legal or trade obligation, purpose, or economic justification;
2. The client is not properly identified;
3. The amount involved is not commensurate with the business of financial capacity of the client;
4. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject or reporting requirements under the Act;
5. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered institution;
6. The transaction is in any way related to an unlawful activity or offense under this Act that is about to be, is being or has been committed; or
7. Any transaction that is similar or analogous to any of the following.

In this regard, the Corporation shall exercise due diligence by implementing adequate systems for identifying and detecting suspicious transactions.

CTR must be done by the Corporation within five (5) working days from the occurrence thereof. Meanwhile, the STR must be reported the next working day.

V. Confidentiality and Tipping-Off

Access to sensitive AML/CTF information is restricted to authorized personnel only, including compliance officers, senior management, and specific employees requiring access for their duties.

Sensitive information is safeguarded through physical, technical, and administrative measures, such as secure storage systems, encryption of digital data, and strict access controls or passwords.

Tipping-off, which could compromise investigations and regulatory actions, is strictly prohibited under AML/CTF regulations, with potential legal consequences including fines and imprisonment for individuals and significant penalties for the organization.

Non-compliance with confidentiality and tipping-off policies is treated seriously, potentially resulting in disciplinary action up to and including termination of employment, and violations may be reported to relevant authorities.

VI. Training and Continuing Education Program

The Corporation shall provide education and training for all staff and personnel, including directors and officers, to ensure they fully understand their personal obligations and responsibilities in combating money laundering and are familiar with its system for reporting and investigating suspicious matters.

The Corporation may assign internal audit or training functions to external parties (e.g., professionals, associations, parent companies, or external auditors). The Corporation exercises due diligence to ensure these parties can effectively perform these functions and notifies the Council in writing of the appointment.

Timing and content of training for various sectors of staff will be adapted by the Corporation as follows:

New Staff: All new employees, regardless of seniority, should receive training on recognizing and reporting suspicious transactions related to money laundering within the Corporation.

Cashiers/Loan and Reloan Officer/Marketing Officer: Personnel directly interacting with the public are crucial in identifying potential money laundering activities. They should be trained to identify suspicious transactions, understand reporting procedures, and be familiar with the Corporation's policies for handling non-regular customers, especially in cases of large cash transactions and suspicious circumstances.

Supervisors and Managers. Supervisors and managers should receive comprehensive training on money laundering procedures, including AMLA offenses and penalties, procedures for service of production and restraint orders, internal reporting procedures, and requirements for verification of identity and retention records.

The Corporation shall arrange annual refresher sessions to remind key staff of their responsibilities and update them on changes in money laundering laws, rules, internal procedures, and Corporation protocols.

VII. Record-Keeping and Retention

The Corporation follows these document retention periods such as:

1. All transaction records, especially customer identification records, are stored securely for five (5) years from the transaction dates.

2. Records of closed accounts, including customer identification, account files, and business correspondence, are kept for at least five (5) years from the closure dates.

3. SRC Rule 52.1 (1) (Books and Records Keeping Rule) and

Rule 52.1 (2) (records Retention Rule) of the Amended Implementing Rules and Regulations of the Securities Regulations Code and continue to be in full force and effect.

Records related to ongoing investigations or transactions disclosed shall be retained beyond the stipulated retention period until the case is confirmed closed.

The Corporation designates at least two (2) persons responsible for record safekeeping, reporting any changes to the Commission.

4. The Corporation shall implement the Digitization of Client Record Program, ensuring all client records and transaction documents are digitized in compliance with AMLC Regulatory Issuance A, B, and C No. 2 Series of 2018, also known as the **Guidelines on Digitization of Customer Records (DIGICUR).**

   The following procedures must be complied:

   1. Branches shall conduct daily scanning of client records before loan release, using prescribed filenames based on document type.

   2. Clear and complete scanned/digitized files shall be uploaded to the File Upload folder in the Loan System.

   3. The Head of the Processing Department and/or Branch Manager must verify the clarity of digitized customer files and transfer them to each branch or business unit folder daily.

   4. The Information Technology Department shall develop and install a program to safeguard digitized customer records.

   5. Approval for access to digitized customer records shall be granted by the Head of the Processing Department, Branch Manager, and designated Records Custodian.

VIII. Third-Party Reliance

The Corporation may utilize third-party service providers for AML and CTF activities under relevant regulations. This practice ensures comprehensive AML/CTF coverage for customer identification, enhanced due diligence, transaction monitoring, and reporting of suspicious activities through specialized expertise and resources.

Before engagement, thorough due diligence is conducted to assess their capabilities, including experience, reputation, regulatory compliance, and internal controls effectiveness.

The Compliance Department of the Corporation, in collaboration with the Board of Directors, is responsible for approving third-party engagements based on due diligence findings and internal approvals.

Termination of relationships may occur if providers fail to meet AML/CTF requirements, perform unsatisfactorily, or breach contractual agreements.

IX. Outsourcing of Conduct of Customer Identification and Due Diligence

The Corporation acknowledges the advantages of outsourcing, such as cost savings and specialized expertise, while also prioritizing strong AML/CTF controls, even when utilizing outsourcing.

Before contracting, the Corporation conducts a thorough risk assessment, considering the nature of the activity, provider reputation, AML/CTF policies, financial stability, and compliance history, but only considering reputable and compliant providers.

Contracts with service providers will define work scope, responsibilities, performance standards, and compliance obligations. The Corporation will establish Service-level agreements ensure ongoing monitoring, with regular audits and reviews.

The Corporation consistently monitors outsourced activities to ensure AML/CTF standards compliance through regular reviews, audits, and reporting.

X. Customer Refusal

In the event that a customer refuses to provide necessary information or cooperate with our due diligence procedures, it is essential for the Corporation to have clear procedures in place to address such refusals while maintaining compliance with applicable laws and regulations.

As part of our commitment to AML/CTF compliance, when a customer refuses to provide required details, the Corporation's staff follows established procedures. This includes documenting the refusal, capturing the specific information or action requested, the reasons provided for the refusal, and any relevant communication with the customer.

Further, the Corporation recognizes that refusal may sometimes be legitimate due to cultural norms or language barriers. However, the Corporation remains vigilant to detect any suspicious patterns. Instances of customer refusal that pose significant risks or raise suspicions of money laundering or terrorism financing are promptly reported to our designated compliance officer or relevant authorities in accordance with regulatory requirements. These reports detail all relevant refusal information and any subsequent actions taken by our company.

XI. Prohibited Accounts

The Corporation is dedicated to prevent the use of its services for money laundering, terrorism financing, and other illicit activities. Prohibited accounts may include anonymous or fictitious accounts, as well as those associated with high-risk jurisdictions.

The Corporation diligently identifies and monitors accounts that fall into the prohibited category. This includes scrutinizing account opening documentation and transaction

patterns, gathering additional information, verifying the source of funds, assessing the purpose of the account, and continuously monitoring prohibited accounts to detect any suspicious activity promptly. Moreover, regular reviews help the Corporation stay vigilant.

XII. Targeted Financial Sanctions (TFS) and TFS Related to Proliferation Financing (PF)

TFS are measures aimed at restricting specific financial activities related to designated individuals, entities, or countries, including asset freezes, travel bans, and trade restrictions.

The Corporation recognizes the importance of complying with TFS to prevent money laundering, terrorist financing, and proliferation financing. Therefore, various TFS measures are implemented as required by relevant authorities to curb illicit financial flows and disrupt the activities of sanctioned parties.

PF involves providing financial support to entities engaged in the proliferation of weapons of mass destruction. The Corporation remains vigilant in identifying and preventing PF-related transactions.

To comply with TFS and prevent PF, the Corporation conducts ongoing monitoring of transactions and promptly report any suspicious activity and cooperate with the AMLC and supervising authorities.

XIII. Cooperation with the AMLC and Supervising Authorities (SAs)

The Corporation recognizes the critical role of cooperation with the AMLC and supervising authorities in combating money laundering and terrorist financing.

The Corporation promptly reports suspicious transactions to the AMLC as required by law and cooperate with supervising authorities during investigations and provide necessary information.

The Corporation maintains open channels of communication with the AMLC and SAs and our designated points of contact ensure timely responses to requests for assistance.

The Corporation's staff undergo regular training on AML/CTF compliance and the importance of cooperation and raise awareness about the impact of our collaboration on the overall financial system's integrity.

PART 4 – FORMS AND TEMPLATES

I. Customer Due Diligence (CDD) Form

SECTION A: PERSONAL PARTICULARS	
Full name:	
Aliases (if any):	
Unique Identification Number (Identity card or passport number):	
Expiry date of identification document (if applicable):	
Nationality (please indicate all nationalities):	
Date of birth:	
Gender (M/F):	
Residential address:	
Telephone number:	
Email address:	

SECTION B: OCCUPATION / BUSINESS DETAILS		
1.	What is your occupation?	
2.	If you are a business owner, please provide details of the industry and business (e.g. products / services).	
3.	In your occupation / business, which are the primary countries in which you have dealings with?	
4.	In your occupation / business, do you deal with any individual or entity from a country or a territory that have dealings with high-risk jurisdiction? If the response to the above is "Yes", please indicate the specific countries and the nature of those dealings.	Yes /No

SECTION C: POLITICALLY EXPOSED PERSON		
1.	Are you a current or former Politically Exposed Person (PEP)? *PEP means that you are an individual who is or has been entrusted with prominent public position in (a) the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (b) a foreign State; or (c) an international organization.*	Yes / No
2.	Are you a "family member" of a current or former PEP?	Yes / No

	"Family member" refers to spouse or partner; children or their spouses or partners; and parents or parents-in-law.	
3.	Are you a "close associate" of a current or former PEP that are reputedly known to have: 1) Joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP; or Page 6 of 23 2) Sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/principal PEP?	Yes / No
4.	If any of the responses in questions 1, 2 and 3 above is "Yes", please complete ***Form C***.	Yes (See Form C) / NA

FORM C: CATEGORIES OF PEP, FAMILY MEMBER OF PEP AND CLOSE ASSOCIATE OF PEP

I am a:

- ☐ PEP
  - ☐ Philippine PEP
  - ☐ Foreign PEP
  - ☐ International Organization PEP
- ☐ Family member of PEP
  - ☐ Parent / Step-parent
  - ☐ Spouse
  - ☐ Child / Adopted child / Step-child
  - ☐ Sibling / Adopted sibling / Step-sibling
- ☐ Close associate of PEP *(please describe relationship with the PEP)*: _____

SECTION D: Declaration by Client or Person Acting on Behalf of Client

I declare that the information provided in this form is true and correct. I am aware that I may be subject to prosecution and criminal sanctions under written law if I am found to have made any false statement which I know to be false or which I do not believe to be true, or if I have intentionally suppressed any material fact.

Signature:	
Name of client / person acting on behalf of client:	
Relationship with client if signed by a person acting on behalf:	
Date:	

FOR OFFICE USE

Verification of client's details

1.	Verify each of the following details obtained in Section A to the original identity card or passport (or other independent and reliable identification document) that bears a photograph of the client: - Full name - Aliases (if any)	Document verified to:	_____ __

	- Identity card or passport (or other identification document) number - Nationality - Date of birth - Residential address The professional firm may consider accepting documents that are certified to be true copies by an independent, qualified person, such as a network firm, a notary public, or an external law firm.	Copy of document retained:	Yes / No
2.	Where the identity card or passport (or other independent and reliable identification document) does not indicate the residential address, verify to other independent and reliable document containing the residential address of the individual (e.g. an original bank statement or recent utility bill).	Document verified to: Copy of document retained:	_____ Yes / No
Screening			
3.	The following details of the client have been screened: - Full name - Aliases (if any) - Identity card or passport (or other identification document) number - Residential address	Yes / No	
4.	Depending on risk assessment, the professional firm may perform further screening on details in (3) above against other information sources and/or other third-party screening database.	Yes / No	
5.	Any exception from (3) and (4) above has been investigated and disposed of appropriately.	Yes / No / NA	
6.	Documentary evidence of the screening performed and results, including any investigation and disposition of exceptions have been retained.	Yes / No	
Identification of PEP			
7.	Search the name (and aliases, if any) of the client against information sources as per the professional firm's policies and procedures, or other third-party screening databases, to determine if the client is a PEP, family member of a PEP or close associate of a PEP.	Yes / No	
8.	Where there is a difference between the client's declaration in Section C and results from (7) above, investigate and dispose of any exception appropriately.	Yes / No / NA	
9.	Documentary evidence of the search performed and results, including any investigation and disposition of exceptions have been retained.	Yes / No	

II. Suspicious Transaction Report (STR) Template

TO: COMPLIANCE OFFICER

Application No./Loan Code: _____

Name: _____ Transaction Date/ Period: _____

Address: _____ Transaction Amount: _____

Name and Address of Person/s Involved (if known): _____

NATURE

- ☐ Application for loan amount beyond applicant's means
- ☐ Payment of large sum with foreign currency (Attach Foreign Currency Form)
- ☐ Large sum fund transfer
- ☐ Amount not commensurate with financial capacity/ business
- ☐ Payment by third party/ multiple checks
- ☐ Source of Fund Doubtful
- ☐ Payment of large sum in cash
- ☐ No proper ID
- ☐ Unidentified Beneficial Owner
- ☐ Others (Please Specify):_____

Reported by: _____ Position: _____Contact No./ E-mail:_____

Date of Reporting:_____ Noted by (Department Head): _____

Reason/s for considering the incident suspicious:
Recommendation from Department Head:

Compliance Officer's Evaluation/ Comment:

Date Received: _____

No grounds exist (state findings) _____

For Endorsement to the Senior Management/Board of Directors

Acceptance and conduct enhanced ongoing monitoring of the account

For reporting to the AMLC

_____ _____

Signature over Printed Name Date

III. Risk Assessment Form

SECTION A: CLIENT'S RISK FACTORS			
	Question	**Response**	
1	Is this a new client?	Yes	No
2	Is the client a company listed on any stock exchange not subjected to disclosure requirements?	Yes	No
3	Is the client a legal person or an entity that cannot hold assets in its own name?	Yes	No
4	Does the client frequently make unaccounted cash transactions to similar recipient(s)?	Yes	No
5	Do the proposed directors/partners/shareholders have prior criminal convictions involved fraud or dishonesty?	Yes	No
6	Is any of the client beneficial owner or its agent a politically exposed person?	Yes	No
7	Are the client's company accounts outdated?	Yes	No
8	Is there any problem obtaining the required information in the relevant form?	Yes	No
9	Can the information obtained be verified by independent and reliable sources?	Yes	No
	The professional firm has performed further screening of details of client, beneficial owner of the client, person acting on behalf of the client, or connected party of the client against other information sources and/or other third-party screening database. Are there adverse news or information arising?	Yes	No

SECTION B: SERVICES / TRANSACTIONS RISK FACTORS				
	Question	**Response**		
1	Has the client given any instruction to perform a transaction (which may include cash) anonymously?	Yes	No	NA
2	Has the client transferred any funds without the provision of underlying services or transactions?	Yes	No	NA
3	Are there unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)?	Yes	No	NA
4	Are there unaccounted payments received from unknown or un-associated third parties for services and/or transactions provided by the client?	Yes	No	NA
7	Is this business relationship being established without any physical meeting?	Yes	No	NA
8	Are there any transactions being performed without any physical meeting?	Yes	No	NA
9	Are the transactions required by the client inconsistent with the professional intermediaries' knowledge on the client's risk profile?	Yes	No	NA

IV. Training Acknowledgement Form

I, _____ acknowledge that I have read and understand the Anti-Money Laundering Trainings. I agree to abide by the principles that were explained in this training. I understand that if I have any questions about the training, materials presented or information not addressed in the training, or if I encounter any problems, it is my responsibility to seek clarification from the designated Human Resources/Department Head.

_____ _____
(Signature of Employee) (Date)

_____ _____
(Human Resources/Department Head) (Signature/Date)

V. *Sanction Screening Form*

Name:	
Section A: Sanctions Exposure *If yes to any of the below questions, please provide more information to the corresponding Section below each question.* **Sanctioned Countries/Jurisdictions: Iran, North Korea, Syria, Cuba, and Crimea, Kherson, Zaporizhzhia, Luhansk and Donetsk Regions in Ukraine**	
1. Do you transact with persons/entities who are of the following (both currently or in the future): • National/ Resident of Sanctioned Jurisdictions/ Regions • Registered/ Operating/ Located in Sanctioned Jurisdictions/ Regions • Sanctioned parties including owned or controlled by sanctioned parties	☐Yes ☐No
2. Do you transact with persons/entities who are of the following (both currently or in the future) indirectly via subsidiaries, representative offices or intermediaries: • National/ Resident of Sanctioned Jurisdictions/ Regions • Registered/ Operating/ Located in Sanctioned Jurisdictions/ Regions • Sanctioned parties including owned or controlled by sanctioned parties	☐Yes ☐No
3. Do you have subsidiaries, representative offices or any related companies which are: • Registered/ Operating/ Located in Sanctioned Jurisdictions/ Regions • Sanctioned parties including owned or controlled by sanctioned parties	☐Yes ☐No
4. Do you have any dealings with Myanmar Military/ Government or entities owned by Myanmar Military/ Government that are Sanctioned directly or indirectly?	☐Yes ☐No
Details of Sanctions Exposure(s) - Additional Information, if any	

Section B: Customer's Confirmation and Acceptance
I/we confirm that all information provided above is correct and true. I/we undertake that I/we will not transact any business or activities through my/our accounts that directly or indirectly involve or benefit any person or entity located in a Sanctioned Jurisdiction/ Region or, with any jurisdiction, state, entity, vessel or individual, designated as a sanctioned entity. I/we shall notify the Corporation immediately if any representation, undertaking or confirmation contained herein, or any information provided, becomes, or is likely to become untrue or inaccurate in whole or in part, at any time. **Name of Individual(s) & Designation:** **Signature(s):** **Date:**

PART 5 – APPROVING AUTHORITY

The Approving Authority holds a critical role in ensuring the MTPP's integrity and compliance. Their responsibilities include reviewing and approving the MTPP, including policies, procedures, and risk assessments; their sign-off signifies alignment with regulatory requirements; they oversee the implementation of the MTPP across the institution; regular monitoring ensures effectiveness and timely adjustments and approving any updates or amendments to the MTPP.

PART 6 – UPDATING

Regular updates to the Corporation's MTPP are essential to maintain its effectiveness. The Corporation adheres to undergo revision at least once every two years and ensure alignment with evolving AML policies and industry trends. The Corporation reviews risk assessments, procedures, and reporting mechanisms, and any relevant updates are promptly integrated into the MTPP. By proactively updating this MTPP, the Corporation enhances its ability to combat financial crimes.

Date of Approval