Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy

Innomp Group Limited

(DATED: March 14, 2025)

Table of Contents

1. Introduction

1.1 Overview

Innomp Group Limited (hereinafter referred to as “the Company”) adheres to strict Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) standards. The purpose of this policy is to prevent the use of the Company's services for the purpose of money laundering, terrorist financing, and any other illicit financial activities. This policy not only aligns with Saint Lucia's legal requirements but also adopts best practices from leading regulatory frameworks such as the United Kingdom’s Financial Conduct Authority (FCA) and the Financial Action Task Force (FATF).

1.2 Commitment to Compliance

The Company is dedicated to maintaining the highest standards of integrity, transparency, and legal compliance. This includes taking a proactive stance on AML/CTF issues, ensuring the Company is not used for criminal activities, and taking immediate action if suspicious activities are identified. The Company is committed to maintaining a robust compliance framework, encompassing all levels of operations from customer onboarding to transaction monitoring.

2. Legal and Regulatory Framework

2.1 Applicable Laws and Regulations

The Company follows the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations prescribed by the government of Saint Lucia, including but not limited to:

- The Money Laundering (Prevention) Act of Saint Lucia
- The Financial Intelligence Authority Act of Saint Lucia
- FATF Recommendations on AML/CTF
- Other relevant directives by the Financial Services Regulatory Authority (FSRA)

While Saint Lucia may not have as stringent Forex-specific regulations, the Company adopts the highest global standards, ensuring full compliance with international expectations of AML/CTF best practices, such as those found in the United Kingdom under the FCA.

2.2 Continuous Monitoring of Regulatory Updates

The Company is committed to reviewing any updates to AML/CTF regulations both locally and internationally. This ensures that the Company's policies evolve alongside the changing landscape of financial regulations.

3. Know Your Customer (KYC) Procedures

3.1 Standard KYC Procedures

The Company undertakes comprehensive KYC procedures for all customers. This includes, but is not limited to:

- Verifying the customer's identity using government-issued identification documents.
- Proof of residence (e.g., utility bills or official government correspondence).
- For corporate clients, acquiring business registration documents and details of the company's beneficial owners.
- Identifying and verifying Ultimate Beneficial Owners (UBOs) to ensure transparency in business dealings.

3.2 Enhanced Due Diligence (EDD)

In cases where customers are deemed high-risk, the Company applies Enhanced Due Diligence (EDD). High-risk customers include, but are not limited to:

- Politically Exposed Persons (PEPs)
- Customers from high-risk jurisdictions
- Customers displaying unusual transaction patterns or with complex corporate structures

3.3 Continuous Monitoring of KYC Data

KYC data is continuously monitored and updated as necessary. In line with international practices, the Company performs regular reviews and takes corrective

action where necessary.

4. Customer Due Diligence (CDD) and Risk-Based Approach

4.1 Risk-Based Approach (RBA)

The Company takes a risk-based approach (RBA) to Customer Due Diligence (CDD). Customers are classified into low, medium, and high-risk categories based on various factors, such as their transaction patterns, business nature, and geographical location.

4.2 Transaction Monitoring and Manual Reviews

Each transaction is carefully monitored for any suspicious activities. For high-risk customers or large transactions, the Company performs manual reviews and assessments to ensure compliance with AML/CTF regulations.

5. Transaction Monitoring and Reporting

5.1 Monitoring for Suspicious Activity

The Company employs automated systems to monitor transactions for unusual or potentially illicit financial activity. This includes the monitoring of:

- Large, unexplained transactions
- High-frequency international wire transfers, particularly to/from high-risk jurisdictions
- Structuring of transactions to avoid reporting thresholds

5.2 Reporting Suspicious Activity

If any suspicious activity is detected, it will be reported to the Financial Intelligence Authority (FIA) of Saint Lucia immediately, in compliance with local regulations and international AML/CTF obligations.

6. Record-Keeping Requirements

6.1 Documentation and Record Retention

The Company maintains accurate and detailed records of customer identification documents, transaction histories, and reports of suspicious activities. These records are kept for a minimum of five (5) years, as required by the applicable regulatory authorities.

7. AML Officer and Compliance Oversight

7.1 Role and Responsibilities of AML Officer

The Company appoints an AML Compliance Officer who is responsible for overseeing the implementation and enforcement of AML/CTF policies and procedures. The AML Officer also ensures the Company's compliance with both local and international regulatory requirements.

8. Employee Training and Awareness

8.1 Mandatory Training Programs

All employees undergo mandatory AML/CTF training to ensure they are aware of potential red flags and understand the necessary steps to take when suspicious activity is detected. Regular refresher courses are held to keep employees updated on changes in regulations and emerging trends in financial crime.

9. Third-Party Due Diligence

9.1 Due Diligence on Third-Party Partners

The Company performs comprehensive due diligence on all third-party partners, including payment processors, correspondent banks, and technology service providers. If any third-party partner fails to meet the Company's AML/CTF standards, the Company will terminate its business relationship with that partner.

10. Non-Compliance and Penalties

10.1 Consequences of Non-Compliance

Failure to comply with this AML policy may result in:

- Immediate termination of employment for staff found in violation
- Termination of business relationships with non-compliant clients or third-party partners
- Reporting of non-compliant activities to relevant authorities

11. THE COMPANY'S ANTI MONEY LAUNDERING (AML) AND COUNTER- TERRORIST FINANCING (CTF) OBLIGATIONS

To maintain the company's integrity and reputation it is important t o identify, report, and take precautions to guard against money laundering and financing of terrorism.

The nature of the Company's business requires it to abide by all of the above-mentioned anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation and regulations.

11.1 In General

In order to prevent the Company's products and services from being used for the laundering of the proceeds of crime, it is required to establish appropriate and proportionate to the level of risk, systems and controls, and ensure their effective implementation, including, without limitation, the following:

a. Identifying our Clients;

b. Identifying, monitoring and reporting any kind of suspicious transactions;

c. Maintaining transaction records for a minimum of seven (7) years after the termination of our contractual relationships with our Clients;

d. Training our staff to recognize suspicious transactions and to fulfil all reporting obligations;

e. Depending on Client location, report any suspicious activities to authorities in several countries where the Company is offering its products and services.

11.2 Client Onboarding And Acceptance

11.2.1 In line with the foregoing, the Company has established the following rules for the 'onboarding and acceptance of Clients':

A. All Clients have to submit a valid 'Proof ofIdentity (POI)', which must be fully legible, colored with full name, surname and clear and identifiable photograph; any of the following may be submitted:

- Client's valid passport,
- Valid National Identification Card,
- Valid Driver's License

B. All Clients have to submit a valid 'Proof of Residence (POR)'; POR must have been issued in the individual's name and must contain the individual's residential address; it cannot be older than three (3) months and cannot be the same as the document provided as proof of identity; any of the following may be submitted:

- Utility bill (electricity or water authority bill, internet or phone services bill);
- Bank statement (current, deposit or credit card account)

C. All Clients are screened against a 'Risk Screening Tool Database', in order to ensure that the identity of the Client in question does not match with any persons who are known to have criminal background or are subject to sanctions, or is associated with banned entities such as individual terrorists or terrorist organizations, etc. In addition, the Clients are screened against records of PEPs (including their close associates and family members), which are also covered in the Risk Screening Tool database;

D. All Clients are classified into different risk categories in line with the provisions of the Client Classification section ofthe Company's AML Manual. The following risk factors, inter alia, are accounted for when considering the level of risk involved with each Client relationship:

- Cumulative amount of funds depositedinto the Client account/accounts;;
- Country of Residence
- Nationality
- Results on risk screening, etc

E. Depending on the level of risk assigned to the Client, additional checks may be required for Clients, falling within higher risk categories; enhanced due diligence is conducted for such Clients, whereby the source of funds and/or source of wealth, and any other information deemed necessary, are verified additionally to the checks conducted within the standard due diligence.

F. Following the necessary checks, and based on the perceived level of risk, associated with each Client relationship, the decision is made to either proceed with a Client's application or reject it. For all the Clients classified as high-risk, an approval from either the Company's 'Money Laundering Compliance Officer (MLCO)', 'Compliance Officer (CO)' or 'Chief executive Officer (CEO)' is required;

G. 'Politically Exposed Persons (PEPs), their family members and close associates are classified as higher risk and must undergo enhanced due diligence procedures.

The FATF's latest definition of'Politically Exposed Persons (PEP)' includes the following:

- **Foreign PEPs**: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of state or Heads of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

- **Domestic PEPs**: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, members of parliament, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

- **PEPs by function**: Persons who are or have been entrusted with a prominent function by a state-owned enterprise or an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.Country of Residence

11.2.2 The screening of all Clients against the applicable UN, US and EU sanctions lists, is an integral part of the screening of Clients against the Company's 'Risk Screening Tool Database'; where a Client is identified as a true match on any of the above sanctions list during the risk screening process, the account opening application of the Client in question shall be rejected and no business activity shall be initiated with such Client.

11.2.3 In line with the foregoing, the following are not accepted by the Company as Clients (the list below is not exhaustive):

a. where sufficient KYC information could not be obtained/confirmed or as per the Client's risk categorization;

b. the Client matches the person in the sanction lists during risk screening and the match is confirmed to be a true match by the designated Compliance Officer (CO) or the Money Laundering Compliance Officer (MLCO);

c. the Client matches the person in the lists with criminal records during risk screening and the match is confirmed to be a true match by the designated Compliance Officer (CO) or the Money Laundering Compliance Officer (MLCO);

d. Clients from countries on the list of non-cooperatives jurisdictions with the FATF;

e. Clients from restricted jurisdictions, as per the list published on the Company's Website(s);

f. Clients whose accounts are in name of companies, the shares of which are in bearer form;

g. Clients whose accounts are in the name of a Trust;

11.3 Ongoing Client Monitoring

The ongoing monitoring of Client relationships is comprised of two sets of measures:

a. All Client records are kept up-to date, KYC information and documents are updated regularly; these updates include, for instance, ongoing risk screening for all existing Clients against the Company's 'Risk Screening Tool Database'; such Client information updates may result in re-classification of the Client into a different risk category, in which instance, the rules for ongoing monitoring over this Client relationship will be reset to align with the updated risk category;

b. Ongoing screening of existing Clients against the Company's 'Risk Screening Tool Database includes screening against the applicable UN, US and EU sanctions lists; in the event that a Client is identified as a true match on any of the above sanctions lists during the ongoing risk screening process, the account of the Client shall be closed, and no further business activity shall be conducted with such Client;

c. The Company's transaction monitoring rules are designed in accordance with the applicable risk classification of a Client relationship; ongoing monitoring of each Client's activity is conducted by the Company's Compliance Officers and Money Laundering Compliance Officers, in "real-time" and retrospectively.

11.4 Internal and External Reporting

11.4.1 Clients should assume that all information provided to the Company is available to the competent regulatory authorities in (a) the country of incorporation of the Company, i.e. the Republic of Seychelles; (b) the country of origin of any funds transmitted to the Company;and (c) the destination country ofany funds refunded by or withdrawn from the Company.

11.4.2 The Company reserves the right to refuse the processing of a transfer of funds at any stage if it believes it to be connected in any way to criminal activities or money laundering.

11.4.3 The Company is obliged to report all suspicious transactions and is prohibited from informing Clients in case they have been reported for suspicious account activity.

11.4.4 As indicated above, any such misuse of an account held withthe Company for money laundering, terrorist financing and/or related offences that is reported to the relevant authorities may result in criminal prosecution.

12. Policy Review and Updates

12.1 Regular Review of Policy

This AML/CTF Policy is reviewed periodically to ensure its alignment with updated local and international regulations, changes in global AML/CTF standards, and emerging financial crime risks.

12.2 Communication of Material Changes

Any substantial changes to the policy will be communicated to stakeholders promptly, and the updated policy will be enforced immediately.

The Company reserves the right to review and/or amend its Money Laundering Prevention Policy, in its sole discretion, whenever it deems fit or appropriate.

Should you have a question about our Money Laundering Prevention Policy please direct your questions to our Support Department: support@innomp.com.