# ZYZ CAPITAL LIMITED

## Anti-Money Laundering & Counter-Terrorist Financing Policy

*International Business Company — Saint Lucia — Reg. No. 2024-00712*

| | |
|---|---|
| **Document title** | Anti-Money Laundering & Counter-Terrorist Financing Policy |
| **Entity** | ZYZ Capital Limited (International Business Company, Saint Lucia) |
| **Registration number** | 2024-00712 |
| **Effective date** | 01-01-2026 |
| **Next review** | Annually, or upon material regulatory change |

## Contents


1. Statement of the Director
2. Purpose and Scope
3. Legal and Regulatory Framework
4. Definitions
5. Governance and Responsibility for AML/CFT
6. Money Laundering and Terrorist Financing
7. Risk-Based Approach and Business-Wide Risk Assessment
8. Risk Matrix and Methodology
9. Know Your Client (KYC)
10. Client Acceptance Policy
11. Client Risk Categorisation
12. Restricted and Prohibited Jurisdictions
13. Sanctions and PEP Screening
14. KYC Documentation Requirements
15. Enhanced Due Diligence
16. Source of Funds and Source of Wealth
17. Ongoing Monitoring and Suspicious Transactions
18. Suspicious Transaction Reporting (STR)
19. Tipping-Off
20. Record Keeping
21. Confidentiality and Data Protection
22. Know Your Employee (KYE) Policy
23. Staff Training
24. Policy Review and Approval


## 1. Statement of the Director

ZYZ Capital Limited, formed under registration number 2024-00712, is governed by its sole Director, who is also the Company's sole ultimate beneficial owner. The Director is responsible for maintaining high standards of corporate integrity and for ensuring that the Company's activities are conducted ethically and in accordance with applicable laws and regulations, thereby supporting long-term stakeholder value and confidence.

The Director has put in place this Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy to set out the controls, roles and procedures by which the Company identifies, prevents and reports money laundering and terrorist financing.

Senior management and all staff are required to read, understand and comply with this Policy and its supporting procedures. Compliance is mandatory, and breaches will be addressed through the Company's disciplinary process.

By adhering to these principles, ZYZ Capital Limited protects its reputation, maintains stakeholder trust and contributes to a safer financial environment.

## 2. Purpose and Scope

This Policy applies to all employees, officers and the Director of ZYZ Capital Limited, and to all business relationships and transactions entered into by the Company. It takes precedence over any conflicting internal instruction, except where a more stringent measure applies.

The purpose of the Policy is to ensure that the Company does not become a conduit for money laundering or terrorist financing, that it meets its obligations under Saint Lucia law, and that it applies a consistent, risk-based approach to client due diligence, monitoring and reporting.

## 3. Legal and Regulatory Framework

ZYZ Capital Limited is incorporated in Saint Lucia as an International Business Company (IBC) under the International Business Companies Act, 1999, and conducts its activities on a cross-border basis through its online trading platform. The Company is not licensed or regulated as a forex or investment-services provider in Saint Lucia, and it does not represent itself as holding any such licence. Its incorporation as an IBC confirms the Company's legal existence; it is not, and should not be read as, a financial-services or brokerage license.

For anti-money-laundering purposes, the Company is subject to the Money Laundering (Prevention) Act and to the supervision of the Financial Intelligence Authority (FIA). The Company observes the following principal legislation:

| Legislation | Relevance |
|---|---|
| **Money Laundering (Prevention) Act, Cap. 12.20 (as amended)** | The principal AML/CFT statute of Saint Lucia. Sets out customer due diligence, record-keeping, suspicious-transaction reporting and related obligations for financial institutions and persons engaged in other business activity. |
| **Financial Intelligence Authority Act, 2002** | Establishes the Financial Intelligence Authority (FIA), the national financial intelligence unit to which suspicious transaction reports are submitted. |
| **Proceeds of Crime Act, Cap. 3.04** | Provides for the identification, tracing, freezing and forfeiture of the proceeds of criminal conduct. |
| **Anti-Terrorism Act, Cap. 3.16** | Addresses terrorist financing offences and related measures. |
| **International Business Companies Act, 1999** | Governs the incorporation and operation of International Business Companies (IBCs), the corporate form under which the Company is incorporated. |
| **Companies Act, 1996 (as amended)** | General companies legislation governing incorporation, directors' duties and corporate matters. |

| Legislation | Relevance |
|---|---|
| **Data Protection Act of Saint Lucia** | Governs the collection, processing and protection of personal data, including data collected for KYC purposes. |

The Company also has regard to relevant international standards, including the Recommendations of the Financial Action Task Force (FATF), and to applicable international sanctions regimes.

## 4. Definitions

- **Money Laundering (ML):** the process of concealing the origins of criminally obtained funds so that they appear to derive from a legitimate source.
- **Terrorist Financing (TF):** the provision or collection of funds, from legitimate or illegitimate sources, intended to be used to carry out terrorist acts.
- **Customer Due Diligence (CDD):** the identification and verification of a client's identity and the assessment of the nature and purpose of the business relationship.
- **Simplified Due Diligence (SDD):** reduced measures applied to demonstrably low-risk relationships.
- **Enhanced Due Diligence (EDD):** additional measures applied to higher-risk relationships, including PEPs, higher-risk jurisdictions and unusual transaction patterns.
- **Beneficial Owner:** the natural person(s) who ultimately own or control a client. For corporate clients, the Company identifies any natural person holding, directly or indirectly, 25% or more of the ownership or voting rights, and any natural person who otherwise exercises control.
- **Politically Exposed Person (PEP):** an individual entrusted with a prominent public function, together with their immediate family members and known close associates (relatives and close associates, or RCAs).
- **Source of Funds (SoF):** the origin of the specific funds used in a transaction or relationship.
- **Source of Wealth (SoW):** the origin of a client's overall wealth.
- **Suspicious Transaction Report (STR):** a report submitted to the FIA where there are grounds to suspect money laundering, terrorist financing or other criminal conduct.

## 5. Governance and Responsibility for AML/CFT

The Company has appointed a dedicated Money Laundering Reporting Officer (MLRO) who is responsible for the Company's AML/CFT framework. The MLRO holds sufficient seniority, authority and independence to discharge the role effectively, has access to all relevant information and resources, and reports to the Director and senior management, who retain overall accountability for the Company's compliance with applicable law.

In this Policy, references to the MLRO mean the individual appointed to that function. The MLRO is responsible for:

- maintaining and periodically reviewing this Policy and its procedures;
- overseeing client due diligence, screening and ongoing monitoring;
- receiving internal escalations of unusual or suspicious activity and deciding whether to file a Suspicious Transaction Report with the FIA;
- maintaining records and the audit trail of AML decisions; and

- arranging staff training and awareness.

Day-to-day identity verification, sanctions and PEP screening are supported by the third-party provider SumSub, and certain operational checks are carried out by back-office staff under the oversight of the MLRO. Where any function is supported by an external provider, ultimate responsibility for compliance remains with the Company and its MLRO; reliance on a third-party tool does not transfer that responsibility.

## 6. Money Laundering and Terrorist Financing

Money laundering is the process of concealing the origins of illegally obtained funds to make them appear legitimate, typically by channeling proceeds of crime through a series of transactions designed to obscure their source. It generally involves three stages:

- **Placement:** introducing illicit funds into the financial system, often through small or structured transactions.
- **Layering:** conducting multiple transactions — such as transfers between accounts or jurisdictions — to obscure the audit trail.
- **Integration:** reintroducing the funds into the legitimate economy through investments, purchases or business activity.

Terrorist financing involves providing funds or resources to support terrorist activity. Unlike money laundering, it may involve funds from legitimate as well as illegitimate sources. Detecting and disrupting both activities is essential to protecting the integrity of the financial system, and the Company applies the controls in this Policy to that end.

## 7. Risk-Based Approach and Business-Wide Risk Assessment

The Company applies a risk-based approach, directing greater resources and scrutiny towards higher-risk clients, products, jurisdictions and delivery channels. Core elements include customer due diligence, transaction monitoring, sanctions and PEP screening, staff training, and clear internal controls and oversight.

The Company maintains a business-wide ML/TF risk assessment that considers its client base, the jurisdictions it serves, the remote (non-face-to-face) nature of onboarding, and its products. The assessment is reviewed at least annually and upon any material change to the business or the regulatory environment, and it informs the calibration of the controls in this Policy.

## 8. Risk Matrix and Methodology

The Company assesses risk by combining the likelihood of an event with its potential impact. Probability is rated as Improbable, Remote, Occasional, Probable or Frequent; impact is rated as Insignificant, Minor, Moderate, Major or Severe. The resulting rating is used to prioritise mitigation and allocate resources.

| Probability \ Impact | Insignificant | Minor | Moderate | Major | Severe |
|---|---|---|---|---|---|
| **Improbable** | Extremely Low | Low | Low | Medium | High |
| **Remote** | Low | Low | Medium | High | Very High |
| **Occasional** | Low | Medium | Medium | High | Very High |
| **Probable** | Medium | Medium | High | High | Critical |
| **Frequent** | High | High | High | Critical | Critical |

## 9. Know Your Client (KYC)

A "client" is any individual, entity or organisation that enters into a business relationship or transaction with the Company. KYC is a core component of the Company's risk management: in addition to establishing a client's identity, the Company monitors account activity to identify transactions that do not conform to the expected profile for that client.

The Company categorises clients to apply proportionate due diligence:

- **Individual clients:** natural persons transacting for personal purposes.
- **Corporate clients:** legal entities transacting for business purposes.
- **Politically Exposed Persons (PEPs):** individuals in prominent public roles (and their RCAs), treated as higher-risk and subject to enhanced due diligence.

The intensity of due diligence — simplified, standard or enhanced — is determined by the client's assessed risk rating.

## 10. Client Acceptance Policy

The Company's Client Acceptance Policy governs the criteria and procedures for onboarding new clients. It applies the following principles:

- **Proper identification:** clients who cannot be properly identified and verified are not accepted.
- **Sanctions and watchlists:** clients appearing on applicable sanctions or watchlists (including the UN, OFAC, EU and UK HM Treasury lists) are not accepted.
- **No anonymous or fictitious names:** the Company does not open accounts in anonymous or fictitious names.
- **Legitimacy of funds and activity:** clients whose funds or activities cannot be verified, or are inconsistent with their profile, are not accepted.
- **Required documentation:** clients must submit the required documentation in acceptable form; failure to do so results in non-acceptance.
- **No involvement in criminal activity:** clients reasonably believed to be involved in criminal activity are not accepted.

On the basis of the assessed risk rating, the Company applies the following acceptance approach:

- **Low risk:** accepted under standard due diligence.
- **Medium risk:** accepted subject to additional KYC documentation and monitoring.
- **High risk:** enhanced due diligence applied; the client may be refused.
- **Unacceptable risk:** refused.

## 11. Client Risk Categorisation

The Company assesses risk factors including geography, business activity, source of funds and transaction patterns, and classifies each client accordingly:

- **Low risk:** no elevated risk factors; the client successfully completed KYC on first submission. Standard due diligence applies.
- **Medium risk:** one or more factors requiring additional verification — for example, low-quality or cropped documents requiring re-submission — or additional documentation at the Company's discretion. Additional monitoring applies.
- **High risk:** significant risk factors, including PEPs and their close associates, clients from higher-risk jurisdictions, or unexplained discrepancies in identity information. Enhanced due diligence and supporting documentation apply, and the client may be refused.
- **Unacceptable risk:** clients prosecuted for financial crime; clients resident in or citizens of jurisdictions subject to FATF increased monitoring or comprehensive sanctions; and clients appearing on terrorist or sanctions lists. Such clients are refused.

Documentation is required to evidence specific fund sources where relevant (for example, proceeds of a property sale or a severance payment). High-risk clients are subject to continuous monitoring and additional verification.

## 12. Restricted and Prohibited Jurisdictions

The Company maintains a documented list of restricted and prohibited jurisdictions, which is reviewed periodically and made available to payment partners and counterparties on request. The Company does not onboard clients who are resident in, or nationals of, jurisdictions that it has designated as prohibited.

In particular, the Company does not accept clients from jurisdictions identified by the FATF as high-risk or subject to increased monitoring (the FATF "black" and "grey" lists), or from countries subject to comprehensive international sanctions. Clients connected with higher-risk jurisdictions that are not prohibited are subject to enhanced due diligence.

The Company provides its services on a cross-border basis from Saint Lucia through its online platform. It does not maintain a local regulated entity, branch, office, agent or representative in the jurisdictions in which its clients reside, and does not hold itself out as locally licensed or authorised where it does not hold such authorisation. Onboarding is in all cases subject to the Company's KYC/AML procedures and to applicable jurisdictional restrictions.

## 13. Sanctions and PEP Screening

The Company uses the third-party KYC and screening provider SumSub to screen clients for exposure to international sanctions (including UN, OFAC, EU and UK HM Treasury lists), politically exposed person status, adverse media, and known or suspected criminal association. Screening is performed before the establishment of a business relationship, before the provision of any service, and before undertaking any transaction for a client, and thereafter on an ongoing basis — including for related entities, directors and beneficial owners.

The Company ensures that its screening arrangements are appropriate to its size and risk profile, that client data used for screening is kept current, and that the configuration and rules of the screening

tool are reviewed periodically. PEP and sanctions screening is carried out on a daily basis against updated lists, irrespective of account activity.

Where a potential match is identified, back-office staff investigate to determine whether it is a true match or a false positive, conducting additional checks using available research and adverse-media sources. Potential matches are referred to the MLRO before any dealing with the person concerned. Upon confirmation of a true match, the MLRO will:

- notify senior management (the Director);
- freeze the relevant account(s) where appropriate;
- maintain a clear, documented audit trail of the investigation, decision and rationale (including the basis for treating any match as a false positive); and
- where necessary, refund and terminate the business relationship, and consider whether a report to the FIA is required.

## 14. KYC Documentation Requirements

### Individual clients

The following information and documents are collected from individual (retail) clients:

- full legal name as shown on the official identity document or passport;
- date and place of birth;
- residential address and country of residence;
- telephone number and e-mail address;
- a clear copy of a valid passport or national identity document; and
- a document evidencing residential address (see below).

### Corporate clients

The following information and documents are collected from corporate or institutional clients:

- full company name, registration number, country of incorporation, registered address, telephone number and e-mail address;
- Memorandum and Articles of Incorporation and Certificate of Incorporation;
- a description of the business, and — for regulated activities — a copy of the applicable licence;
- a list of directors and shareholders and a structure chart of the entity;
- details of the registered office and place of business;
- latest audited accounts, or a signed explanation of their absence (for entities older than two years, director-signed management accounts);
- a Certificate of Good Standing or equivalent;
- a signed and dated board resolution authorising the person acting on the entity's behalf; and
- for each beneficial owner or shareholder holding 25% or more of the voting rights, directly or indirectly, the individual-client documents listed above together with a signed source-of-funds declaration.

### Acceptable proof of identity and address

Identity is evidenced by a high-resolution copy of a passport or national identity document showing the holder's name, date and place of birth, document number, issue and expiry dates, country of issue and signature. For corporate clients, identity is evidenced by documents confirming the entity's existence, such as a Certificate of Incorporation, Certificate of Good Standing and Articles of Incorporation.

Residential (or registered) address is evidenced by one of the following, issued within the last six months: a utility bill (telephone, internet, water or electricity), a bank or credit-card statement, a bank reference letter, a signed tenancy agreement, or a recent tax notification. Expired or illegible documents are not accepted.

## 15. Enhanced Due Diligence

Further documentation, explanation or detail may be required where:

- an account is identified or suspected to be high-risk;
- a client's total deposits exceed USD 75,000; or
- a client's total monthly deposits exceed USD 50,000.

In such cases, ZYZ Capital Limited will:

- seek further information directly from the client, and from independent research or third-party sources, to clarify the nature and purpose of the client's activity;
- obtain supporting documents and complete a source-of-funds / source-of-wealth assessment; and
- apply enhanced ongoing monitoring to the relationship.

PEPs and their close associates are subject to enhanced due diligence in all cases, including senior-level (Director) approval to establish or continue the relationship, establishment of source of wealth and source of funds, and enhanced ongoing monitoring.

A verified profile is created for each client containing all KYC information and submitted documents, stored securely in electronic form on the Company's systems. The profile is reviewed and updated throughout the life of the relationship.

## 16. Source of Funds and Source of Wealth

Where required by a client's risk rating or transaction profile, the Company establishes the source of the specific funds used (source of funds) and the origin of the client's overall wealth (source of wealth). This may include reviewing salary or business income, sale proceeds, inheritance or other documented sources. Relationships where funds or wealth cannot be satisfactorily explained are escalated to the MLRO.

## 17. Ongoing Monitoring and Suspicious Transactions

A suspicious transaction is any activity that departs from a client's usual behaviour or from the expected norms of legitimate business and which may indicate money laundering, terrorist financing or other criminal conduct. The Company monitors activity on an ongoing basis and applies controls

including a transaction-monitoring process, threshold-based alerts, escalation procedures and documented investigation.

Indicators (red flags) that may signal a suspicious transaction include, without limitation:

- transactions that are unusually large, frequent or irregular relative to the client's profile;
- activity inconsistent with the client's known business or stated purpose;
- structuring — splitting transactions to avoid reporting or verification thresholds;
- rapid movement of funds in and out with no apparent economic rationale;
- reluctance to provide, or provision of inconsistent, identifying information;
- involvement of higher-risk jurisdictions, tax havens or parties with weak AML controls;
- payments to or from unrelated third parties;
- funding and withdrawals using different payment methods or instruments, or a mismatch between deposit and withdrawal channels;
- use of multiple payment cards or accounts by a single client, or shared instruments across clients;
- deposits followed by withdrawal with little or no genuine trading activity; and
- elevated chargeback activity or other indicators of payment-instrument misuse.

Identifying a red flag does not by itself establish criminal activity; it triggers investigation by the Company and, where appropriate, escalation to the MLRO.

## 18. Suspicious Transaction Reporting (STR)

Where, following investigation, there are reasonable grounds to suspect money laundering, terrorist financing or other criminal conduct, the MLRO files a Suspicious Transaction Report with the Financial Intelligence Authority (FIA) of Saint Lucia, in accordance with the Money Laundering (Prevention) Act. Reports are made as soon as reasonably practicable and, in any event, within the period prescribed by law.

- **Content:** an STR includes the client's details, the relevant transaction information, and a narrative describing the grounds for suspicion.
- **Confidentiality:** STRs and related information are kept strictly confidential and are not disclosed to the client or to any unauthorised person.
- **Cooperation:** the Company cooperates with the FIA and other competent authorities and acts on any lawful direction received.
- **Obligation:** failure to report suspicious activity may result in penalties for the Company and, potentially, for individuals.

## 19. Tipping-Off

Informing a client, or any other person, that a Suspicious Transaction Report has been or may be filed, or that an investigation is being or may be carried out, is prohibited and may constitute a criminal offence ("tipping-off"). All staff must avoid any action that could prejudice an investigation. Questions about how to respond to a client in these circumstances must be directed to the MLRO.

## 20. Record Keeping

The Company retains all relevant records for a minimum of seven (7) years. Retention applies from the end of the business relationship or the date of the last transaction, as applicable. Records retained include:

- **KYC documentation:** client identification, verification and due-diligence records.
- **Transaction records:** records of all executed transactions.
- **Monitoring and reports:** records of unusual or suspicious activity, internal escalations, and STRs together with supporting documentation.

Records are stored securely in electronic form and are retrievable to support regulatory requirements and lawful investigations.

## 21. Confidentiality and Data Protection

Strict confidentiality is maintained in all aspects of suspicious-transaction management. Information relating to STRs must not be shared with unauthorised parties and is not included in ordinary client files; all AML-related actions are treated as confidential; and the MLRO oversees adherence to these requirements. Breach of confidentiality is subject to disciplinary action and, where applicable, legal consequences.

Personal data collected for KYC and monitoring purposes is processed and protected in accordance with applicable data protection legislation, including the Data Protection Act of Saint Lucia. Such data is used only for compliance and legitimate business purposes, is kept secure, and is retained in line with the record-keeping period set out above.

## 22. Know Your Employee (KYE) Policy

The Company operates a Know Your Employee policy to verify the identity and suitability of each employee. During onboarding, employees provide self-declarations of qualifications, experience and any conflicts of interest, and the Company verifies the authenticity of educational and professional credentials. Employee records are reviewed and kept up to date, and orientation includes training on compliance, ethical conduct and this Policy.

Adherence to the KYE policy forms part of employee performance assessment. Employees are encouraged to report suspicious activity, and the Company protects employees who report concerns in good faith from retaliation. Breaches of the KYE policy — such as providing false information or engaging in deceptive practices — are investigated and may result in counselling, additional training, suspension or termination, following a fair and proportionate process.

## 23. Staff Training

The Company's training programme, overseen by the MLRO, equips staff to understand their legal and regulatory obligations and to recognise and respond to financial-crime risk. Training covers the Company's AML/CFT policies, identification of suspicious activity, the correct reporting procedures (including STRs), data protection, confidentiality and client due diligence, and includes practical scenarios where appropriate.

Refresher training is provided periodically and following material regulatory changes, so that staff remain current and the Company maintains an effective culture of compliance.

## 24. Policy Review and Approval

This Policy is maintained by the MLRO and approved by the Director. It is reviewed at least annually, and additionally upon any material change to the Company's business or to applicable law or regulation. Amendments take effect upon approval by the Director and are communicated to all staff.