Equitex Capital Limited
AML / KYC Policy

October 2026

Review and Approval

The following persons have reviewed and endorsed/approved this document:

Version	Date Reviewed	Reviewed by	Description
1	May 2023	Board of Directors	The Company established and submitted its AML/CFT Manual to the FSA as part of its licence application, in accordance with the AML/CFT Act, 2020 and relevant guidelines issued by the FSA.
2	May 2026	Board of Directors	The Policy is updated to reflect revisions to applicable AML/CFT laws and regulations in force in Seychelles.
3	October 2026	Board of Directors	The Policy is updated to reflect revisions to applicable AML/CFT laws and regulations in force in Seychelles. As well as internal procedures.
4			

DEFINITIONS

Alternate Compliance Officer as per the Anti-Money Laundering and Countering the Financing of Terrorism Act 2020 means a senior official at management level to act as an alternate compliance officer, with the approval of the supervisory authority in the absence of a compliance officer.

AML Act means the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020 as amended;

AML Regulations means the Anti-Money Laundering and Countering the Financing of Terrorism Regulations, 2020, as amended;

Benefit from criminal conduct means any money or property that is derived, obtained or realised, directly or indirectly, by any person from criminal conduct;

Beneficial owner as per the Beneficial ownership Act 2020 means one or more natural persons who ultimately own or control a customer or the natural person or persons on whose behalf a transaction is being conducted and includes those natural persons who exercise ultimate effective control over a legal person or a legal arrangement

BOD means the Board of Directors

Business relationship means the arrangement between a person and a reporting entity whose primary purpose is to facilitate an occasional or regular course of business dealings between them

Cash includes notes and coins of Seychelles or of any other country which is a legal tender and accepted as a medium of exchange in the country of its issue, postal orders, bearer cheques which passes title thereto upon delivery including travelers' cheques, bank drafts and bearer bonds

Customer, in relation to a transaction or an account, includes:

a) the person in whose name a transaction or account is arranged, opened or undertaken;
b) a signatory to a transaction or account;
c) any person to whom a transaction has been assigned or transferred;
d) any person who is authorised to conduct a transaction; or
e) such other person as may be prescribed;

Company means Equitex Capital Limited which is a company incorporated in Seychelles with Company registration number 8434948-1;

Compliance Officer (**CO**) means the appointed person that will perform both duties as per provisions of the Financial Services Authority Act, 2013 and the AML Act.

Criminal conduct shall have the meaning set out in section 3 of AML Act and includes the financing of terrorism;

Data means representations in any form of information or concepts;

Financing of terrorism means any of the offences referred to in sections 5, 6, 7, 8, 9, 10, 12, 15, 16 or 19 of the Prevention of Terrorism Act, 2004;

FIU means the Financial Intelligence Unit of Seychelles, established under section 10 of the AML Act;

FSA means the Seychelles Financial Services Authority;

Law Enforcement Agency means the Financial Crime Investigation Unit or any other Unit as may be designated by the Commissioner of Police within the Seychelles Police Force; the Anti-Corruption Commission of Seychelles; the Department of Immigration; the Seychelles Revenue Commission or any other Agency as may be specified by the Minister by notice published in the Gazette to carry out criminal investigation in Seychelles;

Person includes a body of persons whether it has legal personality or not;

Politically Exposed Person (PEP) means:

a) an individual who is or has been, during the preceding three years, entrusted with a prominent public function in:
    i) Seychelles;
    ii) any other country; or
    iii) an international body or organisation;
b) an immediate family member of a person referred to in (a); or
c) a close associate of a person referred to in (a).

Politically exposed persons include:

a) heads of state, heads of government, ministers and other and senior politicians;
b) senior government or judicial officials;
c) ambassadors and chargés d'affaires;
d) persons appointed as honorary consuls;
e) high-ranking officers in the armed forces;
f) members of the boards of central banks;
g) members of state-owned corporations; and
h) influential political party officials.

Reference to Immediate family members of a person specified in (a) above include:

a) a spouse;
b) a partner, that is an individual considered by his or her national law as equivalent to a spouse;
c) children and their spouses or partners, as defined in this section;
d) parents; and
e) siblings.

Reference to Close associates of a person specified in (a) above include:

a) any person who is known to have joint beneficial ownership of a legal person, partnership, trust or any other close business relations with that legal person, partnership or trust; and
b) any person who has sole beneficial ownership of a legal person, partnership or trust which is known to have been set up for the benefit of that legal person, partnership or trust.

In determining whether a person is a close associate of a person specified in (a) above, a reporting entity shall have regard to public information or such information that the reporting entity has in its possession.

Prevention of Terrorism Act means the Seychelles' Prevention of Terrorism Act 2004 as amended;

Regulated business means a business for which a license is required under the corresponding Act;

Regulatory authority/Supervisory authority means the Financial Services Authority of Seychelles

Republic means the Republic of Seychelles;

Regulations means the regulations made under the AML Act;

Suspicious Transactions Report or Suspicious Activity Report means a report on an activity or a transaction or series of transactions made, to be made or attempted to be made, by a reporting entity under section 48 of the AML Act 2020.

Users Includes any person or entity who registers with the Company.

Commented [TM1]: Please make sure all the terms defined here are included in the document. Those not mentioned in the document should be deleted accordingly.

Commented [sd1R2]: Updated the terms to correspond to the document

AML/KYC Policy

Introduction

Equitex Capital Limited (the "Company") Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML/KYC Policy") is designated to prevent and mitigate possible risks of the Company being involved in any kind of illegal activity.

Equitex Capital Limited is a limited liability company duly incorporated in the Seychelles on 9th of May, 2023, with registration number 8434948-1 and license number SD185. The Company is licensed and regulated by the Financial Services Authority (FSA) under the Securities Act, 2007 to carry on securities dealer activities. The Company recognizes its obligation to prevent its services and systems from being used for money laundering, terrorist financing, or any other financial crime. The Company is committed to conducting its business in full compliance with the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020 (the "AML Act"), the AML/CFT Guidelines, and any other applicable regulations.

Both international and local regulations require Equitex Capital Limited to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, the proliferation of weapons of mass destruction (WMD), corruption and bribery and to take action in case of any form of suspicious activity from its Users.

Commented [TM2]: This terminology should be clearly defined in the definitions section

Commented [TM2R2]: @stamatis, "Users" should be defined in the Definitions page above

Commented [sd2R3]: @Terina I have added a definition in the Definitions page above

Commented [TM2R4]: I moved it to the bottom so that all definitions would be in alphabetical order

The AML/KYC Policy covers the following core AML components:

1. Money Laundering and Terrorist Financing
2. Board of Directors' Roles and Duties
3. Verification procedures
4. Sanctions and PEP lists screening
5. Compliance Officer
6. Monitoring Transactions
7. Suspicious Transaction Report (STR)
8. Risk Assessment
9. Breaches of Anti-Money Laundering/Know-Your Customer Policy

1. Money Laundering and Terrorist Financing

Money laundering is a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Money laundering enables criminals to maintain control over their illicit proceeds and ultimately to provide legitimate cover for the illegal source of the illicit proceeds. This means that proceeds from criminal activities are converted into assets that gives it an appearance of legitimate money. Money laundering is an international scourge and the failure by the authorities to prevent the laundering of the proceeds of crime will enable criminals to benefit from their illegal activities, thereby making crime a viable proposition.

The Financing of Terrorism is defined as an offence established when a person "by means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they will be used in full or in part, in order to carry out a terrorist act or activity". Terrorist financing is a unique form of financial crime. Unlike money laundering which involves money obtained from illicit activities, terrorist financing can be funded from legally obtained funds to be used for terrorist activities.

The three basic stages of money laundering:

a) Placement: is the physical deposit of criminal proceeds derived from illegal activity i.e. entering the collected cash into the financial circuits (payment in cash, exchange of bills, manual exchange, travelers' checks, casino checks, etc.).

b) Layering: is the separation of criminal proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity i.e. transfer between accounts, drawing of checks, foreign transactions etc.

c) Integration: is the provision of apparent legitimacy to the proceeds of crime. If the layering process has succeeded, integration places the laundered proceeds back into the economy in such a way that they appear as normal (business) funds or other assets i.e. investing funds in lawful investments (stores, leisure activities, real estate), but also companies of all types, etc.

Offence of Money Laundering as per the AML Act

A person is guilty of money laundering if:

a) he or she directly or indirectly acquires property from the proceeds of criminal conduct;
b) knowing or believing that property is or represents the benefit from criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on him):
c) converts, transfers or handles the property, or removes it from the Republic;
d) conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or
e) acquires, possesses or uses the property.

Any person who participates in such conduct as described above is considered to commit the offence of money laundering and shall be liable to be punished accordingly.

The person who commits and is found guilty of money laundering is liable on conviction to a fine not exceeding SCR 5,000,000 or to imprisonment for a term not exceeding 15 years or to both; For the same offence a legal person is liable on conviction to a fine not exceeding SCR10,000,000.

2. Board of Directors' Roles and Duties

The Board of Directors is ultimately responsible for ensuring the Company's compliance with the applicable legal and regulatory framework of Seychelles, including the requirements of the AML Act 2020 and related securities laws.

The Board shall:

- Ensure the establishment, implementation, and maintenance of an effective and risk-based AML/CFT framework, including adequate systems, controls, policies, and procedures to identify, assess, monitor, and mitigate money laundering and terrorist financing risks.
- Approve and periodically review the Company's AML/CFT policies and Institutional Risk Assessment, ensuring that measures adopted are appropriate to the nature, scale, and complexity of the Company's activities.
- Determine, record, and approve the Company's AML/CFT policy principles and ensure they are effectively communicated and implemented.

- Ensure full compliance with all applicable AML/CFT legislation and confirm that appropriate, effective, and proportionate controls are in place.
- Approve formally documented AML/KYC policies and ensure they are circulated to all relevant personnel.
- Appoint a Compliance Officer in accordance with the AML Act 2020 and ensure that the officer is provided with sufficient authority, independence, resources, and access to information.
- Receive regular written reports, at least annually, on Compliance, AML/CFT, Risk Management, and Internal Control matters, including confirmation that appropriate remedial actions have been taken to address identified deficiencies.
- Oversee and monitor the effectiveness of the Company's internal control framework to prevent unlawful or unauthorized activities, ensure alignment with the Company's strategy, facilitate risk identification, and maintain timely and accurate information flows.
- Conduct periodic reviews of the overall control environment and the effectiveness of control functions (including Compliance and Internal Audit, where applicable), and assess management's implementation of related recommendations.

The Board retains ultimate accountability for maintaining an adequate, effective, and sustainable system of internal controls.

3. Verification procedures

One of the international standards for preventing illegal activity is customer due diligence ("CDD"). According to CDD, Equitex Capital Limited establishes its own verification procedures within the standards of anti-money laundering and "Know Your Customer" frameworks.

Identity verification

The following outlines the good industry practice when establishing a business relationship or conducting a significant transaction. These steps are designed to ensure full compliance with the Company's CDD obligations and to provide a robust information base for effective ongoing monitoring of clients and their activities:

- The Company adopts a risk-based and technology-driven approach to the identification and verification of clients. This ensures that all customers, whether natural persons or legal entities, are accurately identified and verified before a business relationship is established and throughout its duration. These practices also support the Company's obligation to conduct effective ongoing monitoring and maintain a reliable customer risk profile.

- Records are stored securely in encrypted digital form and are easily retrievable for inspection by the FSA or other competent authorities. Access to client data is strictly controlled, and the Company ensures full compliance with the Data Protection Act, 2023. An electronic audit trail is maintained for every onboarding and verification activity, documenting timestamps, verification actions, and the personnel involved.

- The Company relies heavily on digital onboarding processes. Accordingly, it utilizes secure electronic Know-Your-Customer (e-KYC) systems to verify customer identity remotely. The process involves the submission of official identification documents, such as a valid passport, national identification card, or driver's license, together with a recent proof of address, which may include a utility bill or bank statement dated within the previous three (3) months. Biometric verification tools, such as facial recognition and liveness detection, are used to confirm that the individual submitting the documents is the genuine document holder.

Automated document validation software is employed to detect forgery, tampering, or expired documents.

- As part of its verification procedures, the Company also obtains information on the source of funds used to fund trading accounts and, where appropriate, the client's source of wealth. Where the value or frequency of transactions appears inconsistent with the client's profile, the Company conducts additional verification and may request further explanation or documentation. Clients are required to provide details of the origin of their funds, such as employment income, business proceeds, or investment returns, supported by documentary evidence like bank statements, payslips, or audited financial reports. Third-party payments and deposits from unverified sources are prohibited unless separate due diligence is completed and approved by the Compliance Officer.

- To mitigate exposure to sanctioned or high-risk individuals and entities, the Company screens all clients, beneficial owners, and authorised signatories at onboarding and on an ongoing basis against relevant sanctions lists (UN, EU, UK, and OFAC), FSA circulars, and reputable PEP and adverse media databases. This screening is conducted using automated, real-time systems that update daily. Where a PEP, family member, or close associate is identified, the Company applies enhanced due diligence, including senior management approval and detailed review of the client's source of funds and source of wealth. All screening results, decisions, and supporting documentation are recorded and retained for audit and regulatory inspection.

- To support continued compliance and effectiveness, the Company provides regular AML/CFT training to all employees engaged in client onboarding, verification, and monitoring. The training covers identification procedures, red-flag indicators, suspicious transaction reporting, and updates to regulatory requirements. The Company also performs periodic reviews of its e-KYC vendors and verification systems to ensure they meet industry and regulatory standards.

- In the case of a PEP, the individual that the Company is dealing with should be subject to Enhanced Due Diligence.

- For all prospective Clients, the Company shall obtain the highest-quality identification documents available, including when requested certified translations for any documents not in English. No single form of identification shall be regarded as sufficient to verify the Client's identity. Verification of the Client's residential address is mandatory and shall be treated as an essential component of the identity verification process. For non-face-to-face onboarding, all identity and address verification procedures must be conducted through reliable and independent sources, such as official registries, banks, or licensed verification providers.

- In respect of joint accounts irrespective of whether the surname and/or address of the account holders differ, the identity of all account holders should be verified.

- Where a Client is introduced by a branch or subsidiary of a financial institution located outside Seychelles, provided the identity of the Client has been verified by the introducing branch or subsidiary in line with requirements at least equivalent to those of Seychelles and those identification records are freely and immediately available on request to the reporting entity in Seychelles, it is not necessary for identity to be verified or for the records to be duplicated.

Client identification procedures and Client due diligence measures shall comprise:

Commented [TM3]: Please confirm with company directors if the company will be onboarding PEPs or not. If PEPs are not onboarded, this should be mentioned accordingly - and the AML Manual of the Company will also have to be updated

Commented [TM4]: Same comments as above regarding PEPs

Natural Persons

i) **Proof of Identification**
The full names used should be verified by reference to a document obtained from a reputable official source which bears a photograph. A current valid full passport or national identity card, not older than 10 years, should be requested and the number registered. After the Company is satisfied with the proof of identification it shall keep copies of the pages containing all relevant information.

ii) **Proof of Residential Address**
The Company may obtain one of the following documents to verify the client's residential address:

- A recent utility bill (not older than three (3) months);
- Telephone bill, bank or other financial institution statement (not older than three (3) months);
- Insurance policy which includes a residential address (to guard against forged or counterfeit documents care should be taken to check that the document is original);
- Checking an official register such as the electoral roll;
- Rental agreement;
- Written confirmation from the person's employer.

iii) **Other information**
The following minimum information shall also be obtained from clients that are natural persons:

- Full legal name(s) as stated on the official identity card or passport;
- Permanent residential address;
- Date and place of birth;
- Nationality or citizenship;
- Occupation details;
- Purpose and intended nature of the business relationship;
- Source of funds.

It is not acceptable to rely on the same document or information for both identity verification and residential address verification. The Company shall ensure that separate and independent documentation or procedures are used to verify the client's identity and to confirm their residential address.

Legal Entities
To verify the identity and legal status of a client that is a legal entity, the Company shall obtain and verify the following documents, as applicable:

- Certificate of Incorporation or Certificate of Registration;
- Memorandum and Articles of Association (or equivalent constitutional documents);
- Register of Directors and Register of Shareholders/Members;
- Certificate of Good Standing (where applicable);
- Recent extract from the Company Registry or equivalent independent source;
- Business licence or equivalent authorisation to operate;

- Evidence of the entity's registered office address and principal place of business (e.g. recent utility bill, lease agreement, or bank statement not older than three months); and
- Latest audited financial statements or other evidence of ongoing business activity.

The Company shall also identify and verify the beneficial owners and authorized representatives of the Company by obtaining:

- Valid government-issued photo identification (e.g. passport, national ID card, or driver's license);
- Proof of residential address (e.g. recent utility bill, bank statement, or government correspondence not older than three (3) months); and

Document demonstrating authority to act on behalf of the entity (e.g. Board Resolution, Power of Attorney, or Letter of Authorisation, Assessment Questionnaire with associated scoring)

As part of the KYC onboarding procedure, each client must complete the full Assessment Questionnaire prior to being fully verified. Based on the Client's responses, a numerical risk score is assigned in accordance with the Company's internal risk-scoring methodology. The risk classification assigned to a client determines the level of due diligence, monitoring frequency, transaction review thresholds and approval requirements applicable to the business relationship. Clients classified as High Risk shall be subject to Enhanced Due Diligence (EDD) and ongoing monitoring measures, including but not limited to senior management approval, source of funds verification, enhanced transaction monitoring, and more frequent periodic review.

The resulting risk score determines the Client's risk classification, which may include the following categories:

- Low Risk
- Medium Risk
- High Risk

Clients who have yet to complete the required questionnaire or any other mandatory KYC requirements shall not be assigned a final risk classification and shall not be fully onboarded and shall not be permitted to deposit, withdraw, or execute any transactions or permitted to access trading services until full completion. Such Clients who are still pending a risk categorization shall be classified for internal monitoring purposes as:

- Medium Risk

Clients who are identified as prohibited, restricted, or otherwise unacceptable in accordance with the Company's internal policies shall be classified as:

- Blacklisted

Blacklisted clients cannot appeal their status. The BOD will be notified via email for every client who is classified as Blacklisted.

Commented [TM5]: Elaborate on who approves High risk clients and PEPs. (Note any form of documentation for the escalation procedures should be saved by the Company in case requested by the regulatory authority)

Commented [TM5R2]: You did not mention who will approve High risk clients and PEPs

Commented [sd5R3]: @Terina 'senior management approval' is for High Risk clients.

for PEPS, we do not onboard clients that are PEPs

Joint Accounts

A joint account is made between 2 clients. Both clients should be fully verified and must pass sanctions and PEP screening in order to proceed with the approval.

Once the Internal Back Office & Compliance Officer receives the internal Joint Account Application Form, it then needs to be checked if it is filled and signed by both clients.

- Married Couples – Proof of marriage is required
- 1st Degree Family Related – Proof such as a birth certificate is required
- Non-related but having a joint bank account – Joint bank account statement is required and proof of relationship

In most cases, both account holders will submit the documents mentioned above for individuals. Each individual holding the Joint Bank Account will be independently risk – assessed before being approved, with no contribution percentage required from each client. If additional documents are required, the client will be contacted via email.

- In the event of a high – risk alert, the whole account will be assessed.
- In the event of a withdrawal request – the company will not require dual authorization for the release of funds.

Documents required – Source of Funds

- Payslip
- Contract of Employment
- Tax Declaration
- 12 month bank statement
- Proof savings or fixed deposit certificate
- Sale contract settlement
- Loan Agreement and the bank statement showing the credited funds

Further clarifications

- All documents must show the full name of the clients and relevant amounts.
- Screenshot, PDF's must be clear.
- The Origin of the funds should be consistent with the amount requested

Card verification

The Users who are intended to use payment cards in connection with the Equitex Capital Limited's Services must pass card verification in accordance with Company's policy.

4. Sanctions and PEP lists screening

Equitex Capital Limited screens applicants against recognized Sanctions and Politically Exposed Persons (PEPs) lists. Individuals and legal entities are screened against mentioned lists:

• On the onboarding stage when the user is submitting the application.

• On each anti-fraud and AML alerts manually by the Compliance Officer.

• Daily by running automatically with a script to re-check all Data Base (DB) of customers.

• Any client record/documentation is being uploaded and saved in our CRM

For the screening process Equitex Capital Limited uses Sumsub for the screening and verification of its clients. Any positive match on compromised persons, including but not limited to:

- UN Consolidated List
- EU Consolidated Financial Sanctions List
- OFAC SDN List
- UK HMT Sanctions List
- Politically Exposed Persons (PEP)

Are automatically rejected and manually re-checked by the back office and compliance departments for confirmation.

5. Compliance Officer

Obligations of the Company under Applicable Legislation

The Company shall ensure ongoing compliance with all applicable local laws, regulations, and obligations under the Financial Services Authority Act, 2013(the "**FSA Act**") and the AML Act.

In this respect, the Company shall at all times appoint an individual approved by the FSA to serve as its Compliance Officer. The Compliance Officer shall be responsible for overseeing and ensuring the Company's compliance with:

a) Section 23 of the FSA Act and Section 34 (1) and 34(3) of the AML Act or any other applicable financial services legislation; and
b) Any codes, directives, guidelines or circulars issued by the FSA that are applicable to the Company.

The Compliance Officer shall be approved by the FSA only if they are satisfied that the individual is a fit and proper person to hold such position, in accordance with the applicable regulatory standards and criteria prescribed by the FSA.

Obligations of the Compliance Officer

The Compliance Officer is the person, duly authorized by Equitex Capital Limited, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of Equitex Capital Limited's anti-money laundering and counter-terrorist financing, including but not limited to:

a) identify, assess, advise on, monitor and report on the Company's compliance with regulatory requirements and the suitability of its internal procedures on an on-going basis to the Board and to the respective supervisory authority;

b) be responsible for the implementation and ongoing compliance of the Company's internal programmes, controls and procedures in relation to its business with the requirements of the AML Act;
c) be responsible for ensuring that the staff of the Company comply with the provisions of the AML Act and any other laws relating to money laundering and terrorist financing activities;
d) to receive and review reports of suspicious transactions or suspicious activities made by the staff of the Company and, if sufficient basis exists, report the same to the FIU in accordance with the AML Act;
e) to act as liaison officer between the Company, the supervisory authority (i.e. FSA), and the FIU in the matters relating to money laundering, and terrorist financing activities and for compliance with the provisions of the AML Act;
f) to participate in all mandatory anti-money laundering and countering the financing of terrorism trainings provided by the FSA and the FIU;
g) to identify, assess, advise on, monitor and report on the Company's compliance with regulatory requirements and the suitability of its internal procedures on an ongoing basis to the Board or senior managers and to the FSA upon request;
h) to ensure that the Company maintains a manual of compliance of the policies, procedures, and systems:
    i) with a compliance framework, which shall be submitted to the FSA for review, upon request;
    ii) with all relevant anti-money laundering and countering the financing of terrorism legal and regulatory obligations of the Company and the processes to allow the staff to report violations confidentially to the CO; and
    iii) identifying the procedures to be followed when there have been breaches or suspected breaches of regulatory requirements or internal policies;
i) to ensure compliance by staff of the Company with the provisions of the manual of compliance maintained under paragraph (g) and the non-compliance of the provisions of the manual shall be recorded, showing the nature, form and period of non-compliance and such non-compliances shall be made available to the onsite examiners of the FSA, for examination.
j) to develop a compliance culture:
    i) to ensure that all directors and relevant staff are familiar with the laws and regulations of Seychelles to combat money laundering and terrorist financing activities, which includes an understanding of the relevant compliance policies, procedures and systems of the Company
    ii) where the CO promotes awareness of the need for compliance, thereby developing within the Company a robust compliance culture;
    iii) to monitor the developments and changes in the legislations, policies, standards and other guidelines issued by the international bodies in order to keep the Company updated with the regulatory developments and changes in international requirements;
k) to implement a training programme:
    i) for directors and relevant staff which includes the training programme on general anti-money laundering and countering the financing of terrorism awareness, client acceptance procedures, know your customer (KYC) procedures, remediation and suspicious activity reporting relevant to the Company's activities;
    ii) at least once in every year and whenever there are changes in the laws, regulations or international requirements to ensure that the directors and related staff are aware of the latest developments in the anti-money laundering and countering the financing of terrorism activities;

iii) to undergo additional training, in order to enhance their professional skills, at least once a year;

l) to provide advice and guidance to the employees of the Company on subjects related to anti-money laundering and countering the financing of terrorism;
m) to perform review of the compliance framework and make regular assessment reports to the senior management, identifying the deficiencies and making recommendations for any updates or revisions;
n) to ensure the Company conducts self-assessment of its compliance framework and institute any necessary updates or revisions and make available the self-assessment report to the FSA, upon request;
o) ensure the preparation and submission of an Annual Compliance Report to the FSA for information within ninety (90) days after each calendar year;
p) to maintain a registry with documentation related to the submission, evaluation and escalation of suspicious reports;
q) to maintain a registry of all relevant documentation that verify the accomplishment of the duties of the Company and the Compliance Officer;
r) to ensure the implementation of the procedures described in the Company's Internal Operations Manual;
s) to communicate to all members of staff, the updated copies of Internal Operations Manual, internal regulations and any further instructions and rules in respect to their role and responsibilities in the Company;
t) to provide oversight of the complaints handling process and ensure alignment with regulatory requirements and internal policies; and
u) to review the Company's procedures for preparing and approving marketing communications to ensure compliance with local regulatory requirements.

In the absence of the Compliance officer, the Alternate Compliance Officer will have the above responsibilities when it comes to the duties and responsibilities of the Compliance Officer as per the AML Act.

6. Monitoring Transactions

The clients are known not only by verifying their identity but, more importantly, by analyzing their transactional patterns. Therefore, Equitex Capital Limited relies on data analysis as a risk assessment and suspicion detection tool. Equitex Capital Limited performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include:

1) Daily check of Users against recognized "blacklists" (e.g. OFAC, UN Consolidated List, EU & UK Sanctions Lists), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable.

2) Case and document management.

With regard to the AML/KYC Policy, Equitex Capital Limited will monitor all transactions using a risk-based approach, and it reserves the right to:

- ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer.
- request the client to provide any additional information and documents in case of suspicious

transactions.

- suspend or terminate Client's Account when Equitex Capital Limited has reasonable suspicion that such client engaged in illegal activity.
- Case Retention period is minimum 7 years under the applicable law.

The above list is not exhaustive, and Transaction monitoring is conducted through and supported by manual review. We analyze questionnaire answers to determine economic profiles and monitor for transactions outside of the established patterns. Transactions that fall outside of their regular pattern or are otherwise inconsistent with the economic profile of the client are reviewed by the Compliance Officer. Where suspicion remains following initial review, the matter is escalated to the Compliance Officer for determination as to whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide. Then, a Suspicious Transaction Report (STR) shall be filed with the competent Financial Intelligence Unit (FIU).

7. Suspicious Transaction Report (STR)

Equitex Capital Limited, in line with the international requirements, has adopted a risk-based approach to combating money laundering, terrorist financing and other related financial crime risks. By adopting a risk-based approach, Equitex Capital Limited is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks.

The Company is required by Section 48 of the AML Act to make a suspicious transaction report (STR) in any situation in which the Company:

a) has knowledge or reasonable grounds to suspect that any service or transaction may be related, directly or indirectly, to the commission of criminal conduct (as defined in section 3 of the AML Act, including but not limited to money laundering or terrorist financing);

b) has knowledge or reasonable grounds to suspect that any money or property is or represents
the benefit of criminal conduct;

c) has information that may be relevant to an act preparatory to an offence or to money or property that is or represents the benefit of criminal conduct;

d) has information that may be relevant to an investigation or prosecution of a person for criminal conduct; or

e) has information that may be of assistance in enforcing the AML Act.

The Company shall also consider filing an STR under section 43(3) of the AML Act or a disclosure under section 34 or 35 of the Prevention of Terrorism Act in situations in which the Company:

a) is unable to carry out CDD in accordance with the AML Regulations for any one of its clients; or

b) is unable to undertake ongoing monitoring of any business relationship.

The Company's risk assessment framework forms an integral part of, and operates in conjunction with, its Client Services Agreement, AML Policy, Privacy Policy, Deposit Bonus Terms & Conditions, Refer a Friend Promotion, Terms & Conditions, Partner Agreement, and Swap-Free Account Terms. These documents collectively establish the contractual, operational and compliance controls applicable to Clients and business partners. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

The Company reviews and updates its risk assessment methodology periodically and whenever material changes occur in its products, services, geographic exposure, regulatory obligations, or risk environment.

8. Filing of an STR with the FIU

Where the Compliance Officer/MLRO determines, following an evaluation of an Internal Suspicion Report, that there are reasonable grounds for suspicion of money laundering or terrorist financing, the Company shall submit an STR to the Financial Intelligence Unit (FIU).

The STR must be submitted within two (2) business days of:

- Ascertaining reasonable grounds for suspicion; or
- Receiving the information that gives rise to the suspicion,

whichever occurs first.

It is essential that all relevant fields of the STR form are accurately completed, that the core reason for suspicion is clearly explained, and that the form is dated and authenticated by the Compliance Officer.

The Company shall submit a suspicious transaction report to the FIU within two (2) business days of ascertaining the reasonable grounds, forming the suspicion or receiving the information as set out in the procedures below. It is essential that all relevant fields are completed, that the core reason for the suspicion is explained in detail, and that the form is dated and authenticated.

9. Risk Assessment

Purpose of Risk Assessment

In order to prevent money laundering and combat the financing of terrorism, the Company adopts the following risk assessment methodology on a risk-based approach for the overall assessment of its ML/TF risks and the proper risk management. The risk assessment assists the Company in identifying ML/TF and other illicit financial activity risks and in developing appropriate internal controls (i.e., policies, procedures, and processes). Understanding its risk profile enables the Company to better apply appropriate risk management processes to mitigate and manage risk and comply with regulatory requirements. The risk assessment process also enables the Company to better identify and mitigate any gaps in controls.

The development of the risk assessment generally involves the determination of inherent risks faced by the Company through the identification of specific risk categories (e.g., products, services, customers, geographic locations, customer due diligence carried out by third parties, and technological developments) and the assessment of the quality of the existing AML/CFT controls in order to determine the operating effectiveness of the controls in managing the identified risks.

Risk Factors

The Company has adopted a risk assessment process that takes into account its size, nature, complexity, scope of business activities, and overall risk profile. The determination of inherent AML/CFT risks is based on the following risk parameters, with weightings applied in line with the Company's risk profile:

a) Customer Risk
b) Product/Services & Transaction Risk
c) Geographic Risk
d) Delivery Channel Risk
e) Customer Due Diligence Carried Out by Third Parties
f) Technological Developments.

10. Breaches of Anti-Money Laundering/Know-Your Customer Policy

Any breaches of the Anti-Money Laundering rules will be recorded on the Company's breach log, reported to the Compliance Officer on a monthly basis, and to the Financial Services Authority on a quarterly basis.