1. INTRODUCTION

The Policy on Know Your Customer ("KYC") Norms and Anti-Money Laundering Measures ("Policy") is approved by the Board of Directors of ViewTrade International IFSC Private Limited ("VTI IFSC" or "the Company"), in compliance with International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022.

The Company shall adopt all the best practices prescribed by the International Financial Services Centres Authority ("IFSCA") from time to time and shall make appropriate modifications if any necessary to this Policy to conform to the standards so prescribed. This Policy is applicable across all business segments of the Company and is to be read in conjunction with related operational guidelines issued from time to time. The contents of the Policy shall always be read in tandem/auto- corrected with the changes/modifications prescribed by the IFSCA from time to time.

The Company, by adopting this Policy, endeavours to frame a proper policy framework on 'Know Your Customer' and Anti- Money Laundering ("AML") measures. The Company is committed for transparency and fairness in dealing with all stakeholders and in ensuring adherence to all laws and regulations. The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulge any details thereof for any purpose other than for which the customer has consented to or as required/allowed under applicable laws and regulations. The Company commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is inconformity with applicable laws issued in this regard.

The Company shall ensure that the implementation of the KYC norms is the responsibility of the entire organisation. The Company's Board of Directors and the management team are responsible for implementing the KYC norms hereinafter detailed, and also to ensure that its operations reflect its initiatives to prevent money laundering activities.

2. OBJECTIVE

The objective of this Policy is for VTI IFSC to know / understand its customers and their businesses (if any) thereby allowing the Company to manage its AML and countering of terrorist financing ("CFT") programme prudently. It also prevents the Company from being used, intentionally or unintentionally, by criminal elements for money laundering and other illicit activities. VTI IFSC endeavours to ensure compliance and adoption of KYC/AML/CFT regulations by all its directors, and employees, by means of this Policy.

3. KEY DEFINITIONS

Act	Prevention of Money Laundering Act, 2002
Authority or IFSCA	International Financial Services Centres Authority established under sub section (1) of section 4 of International Financial Services Centres Authority Act, 2019
Beneficial Owner	Shall have the same meaning as ascribed to the term in International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022
Certified Copy	Comparing the original officially valid document provided by the customer with the copy thereof and recording the same as true copy by the Company. Provided that in case of non-resident individuals including Non-Resident Indians (NRIs), the certification may be carried out by: a) Authorised official of a bank located in a Financial Action Task Force ("FATF") compliant jurisdiction with whom the individual has banking relationship b) Notary Public (outside India) c) Court Magistrate (outside India) d) Judge (outside India) e) Certified public or professional accountant (outside India) f) Lawyer (outside India). g) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or h) Any other authority as may be specified by the Authority.
Customer Due Diligence ("CDD")	Identifying and verifying the customer and the Beneficial Owner using 'Officially Valid Documents' as a 'proof of identity' and a 'proof of address' in the manner provided under this Policy read along with the manner prescribed under the IFSCA's Guidelines (*defined below*), as amended from time to time.
Designated Director	A person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the Act, the Rules and Guidelines
End Client	An individual or non-individual that maintains an account or is a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person engaged in the transaction or activity, is acting.
Financial Intelligence Unit or FIU-India	A national agency, set by the Government of India, which is inter-alia responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions.
Guidelines	International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022.
International Financial Services Centre (IFSC)	Shall have the same meaning assigned to it under clause (g) of sub section (1) of section 3 of the IFSCA Act, 2019.
Introducing Firm	A regulated entity that operates as an introducing firm for End Clients to avail the services of the Company through technological integrations with the Company.
Officially Valid Document (OVD)	Passport, Driving License, Proof of possession of Aadhar number, Voter's Identity Card issued by the Election Commission of India or letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the relevant regulator.

	In IFSC, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document. In case simplified measures are adopted by the Company for identification of End Clients where allowed by the Guidelines, the following shall be deemed to be OVD for proof of identity: -Identity card with applicant's photograph issued by Central/ State government departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions - Letter issued by a gazetted officer, with a duly attested photograph of the person. In case simplified measures are adopted as mentioned above, the following shall be deemed to be OVD for proof of address: -Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill) -Property, Municipal tax receipt, city council tax receipt, or such other equivalent document -Post Office savings bank account statement or statement of a bank account including of a foreign bank. -Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address. -Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation. In case the OVD, presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. Where the End Client submits his proof of possession of Aadhaar number as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authority of India.
Politically Exposed Person (PEP)	Individuals who are or have been entrusted with prominent public functions by any country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or international organisations.
Principal Officer	An officer designated by the Company who shall be responsible for furnishing information as required under rule 8 of the Rules.
Rules	Prevention of Money laundering (Maintenance of Records) Rules, 2005
Words and expressions used but not defined in this policy shall have the same meaning as assigned to them under the International Financial Services Centres Authority Act, 2019, the Act, Rules and Guidelines or any regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance. The words customer and client have been used inter changeably in this Policy.	

4. ROLE OF INTRODUCING FIRMS OR THIRD PARTIES

The Company shall implement the KYC norms and AML measures as set out in this Policy for all End Customers who have an account-based relationship with it and/or which have a business relationship with the Company. Where the End Customer has an account with an Introducing Firm, the Company shall ensure that its Introducing Firms undertake regulatory risk-based customer due diligence and KYC in a manner as required under applicable laws and in a manner satisfactory to the Company. The Company may rely on the KYC undertaken by such Introducing Firms or other third parties subject to complying with the following conditions:

It obtains records or information of the Customer Due Diligence conducted by the Introducing Firm within 2 (two) days.

take adequate steps to satisfy itself that the copies of identification data and other relevant documentation relating to the Customer Due Diligence are made available to it by Introducing Firms upon request without delay;

it is satisfied that the Introducing Firm is regulated, supervised, or monitored for, and has measures in place for compliance with Customer Due Diligence and record-keeping requirements prescribed by the FATF;

ensure that the Introducing Firm is not based in a country or jurisdiction assessed as high risk;

ensure that the Introducing Firm has been specifically precluded by the Authority from relying upon for KYC purposes;

(i) it documents the basis for its satisfaction that the requirements set out in point (ii) above.

301B In Brigade International Financial Centre, 3rd Floor, Building No. 14A, Block-14, Zone 1 Gift City
Gandhinagar GIFT SEZ, Dist. Gandhinagar – 382050, Gujarat, India

5. RISK MANAGEMENT

Business Risk Assessment

The Company shall take into consideration the nature, size and the complexity of its business activities and take suitable steps to identify its exposure to money laundering and terrorist financing risks. Further, the Company shall consider the following risk factors, to the extent applicable and relevant, while identifying and assessing the money laundering and terrorist financing risks:

a) its type of customers and their activities;
b) its business engagement with the countries or geographic areas;
c) its products, services, delivery channels and activity profiles;
d) the complexity and volume of its transactions;
e) the development of new products and new business practices, including new delivery mechanisms, channels, and partners; and
f) the use of new or developing technologies for both new and pre-existing products;

Based on the assessment and risk identification made from the above, the Company shall undertake commensurate mitigation measures.

Customer Risk Assessment

The Company shall classify customers into various risk categories. For the purpose of risk categorisation of customer, Company shall obtain the relevant information from the customer at the time of account opening and at any time as and when the Company deem fit. The Company shall have a risk-based approach which includes the following:

a. Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of the Company.
b. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, -information about the clients' business, security offered and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Above parameters will also be considered for Introducing firms.

c. For the purpose of risk categorization of customers, the Company shall follow the following table:

High risk	Medium risk	Low risk
High net worth individuals without an occupation track record of more than 1 years	Salaried applicant with variable income/ unstructured income	Salaried employees with well-defined salary structures and working with public/private limited company. Professionals (Doctors, CAs)
Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations	Self-employed professionals other than HNIs	People working with government owned companies, regulators and statutory bodies, etc.
Firms with sleeping partners	Self-employed customers with sound business and profitable track record for a reasonable period	People whose accounts show small balances and low turnover
Politically exposed persons (PEPs) of Indian/ foreign origin	High net worth individuals with occupation track record of more than 3 years	People working with Public Sector Units) People working with reputed Public Limited
Person with dubious reputation as per public information available	New Client (up to 3 months) in Broking industry	Companies and Multinational Companies, LLPs .

However, above matrix is non-exhaustive and the Company reserves right to assign risk on case-to-case basis, taking into accounts all facts and circumstances.

Further when undertaking an assessment of a customer as mentioned above, the Company shall:

identify the customer and Beneficial Owner, if any;

obtain information on the purpose and intended nature of the business relationship;

obtain information on, and take into consideration, the nature of the customer's business;

take into consideration the nature of the customer, its ownership, control structure, and its Beneficial Ownership, wherever applicable;

take into consideration the nature of the customer's business relationship with the Regulated Entity;

301B In Brigade International Financial Centre, 3rd Floor, Building No. 14A, Block-14, Zone 1 Gift City
Gandhinagar GIFT SEZ, Dist. Gandhinagar – 382050, Gujarat, India

take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;

take into consideration the relevant product, service, or transaction; and,

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company will obtain senior management approval in such cases to continue the business relationship with such person, and also undertake enhanced due diligence and monitoring.

Additionally, to keep the risk assessments up to date, the Company shall review its risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier. The outcome of the exercise shall be put up to the Board of Directors or such other committee of the Board of Directors to which such function has been delegated.

6. CUSTOMER DUE DILIGENCE (CDD)

The Policy approved by the Board of the Company spells out the Customer Due Diligence to be carried out at different stages i.e. with respect to new customers while establishing a business relationship or carrying out a financial transaction or with respect to an existing customer, when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data or where there is a risk of money laundering or terrorist financing or where there is a change in risk-rating of the customer, or it is otherwise warranted by a material change in circumstances of the customer.

Identification of Customers

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship.

An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the Annexure-A.

Verification of Identity of Customers

The Company shall verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person, the Company shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information. The indicative list of documents that the Company may rely on for the purpose of verifying the identity of customers where the customer is an individual or a legal person has been set out in Annexure-A below.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company, shall at their option, rely on customer due diligence done by a third party including Introducing Firms in the manner set out in paragraph 4 above or rely on the records or the information retrieved from the Central KYC Records Registry.

Identification and verification of Beneficial Owners

Where a customer is a natural person or legal person and appoints one or more natural persons to act on its behalf for establishing business relations with the Company and for opening an account of a legal person who is not a natural person, the Company has to identify the beneficial owner(s) and shall undertake all reasonable steps to verify his/her identity. "**Beneficial Owner(s)**" with respect to different types of legal persons shall mean the type of natural persons identified in the table below:

Sr. No.	Customer	Identification
a.	Company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
"Controlling ownership interest" means ownership or an entitlement to more than 10% of the shares or capital or profits of the Company. "Control" shall include right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.		
b.	Partnership firm	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10% of capital or profits of the partnership.
c.	Unincorporated association or Body of Individuals (including societies)	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of or entitlement to more than 15% of the property or capital or profits of the unincorporated association or body of individuals.
Where no natural person is identified under clause (a) to (c), the beneficial owner is the relevant natural person who holds position of senior managing official.		
d.	Trust	The beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

The Company may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

301B In Brigade International Financial Centre, 3rd Floor, Building No. 14A, Block-14, Zone 1 Gift City
Gandhinagar GIFT SEZ, Dist. Gandhinagar – 382050, Gujarat, India

Unless the Company has doubts about the veracity of the Customer Due Diligence information, or suspects that customer may be connected with money laundering or terrorist financing, identification and verification is not required in following cases:

a) Where the client or the owner of the controlling interest is an entity listed on the stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities and such other entities who have been excluded from the requirements regarding identifying and verifying beneficial owners of a customer under the Act and Rules.

b) In cases where a customer is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction.

(Jurisdictions notified by central government: United States of America, Japan, South Korea, United Kingdom excluding British Overseas Territories, France, Germany, Canada)

If the ownership or control arrangements of a customer are of such a nature that the Company is prevented from identifying the Beneficial Owners, the Company shall not establish a business relationship with the customer.

Accounts of Politically Exposed Person (PEP)

The Company shall implement appropriate internal risk management systems, policies and procedures to determine if a customer or any natural person appointed to act on behalf of the customer, or any Beneficial Owner of the customer is a politically exposed person (PEP). In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain senior management approval to continue the business relationship and subject the account to the CDD measures applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

The Company shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a customer or any beneficial owner of the customer is determined by the Company to be a PEP:

a) Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family members, any beneficial owner and close relatives
b) Verify the identity before accepting the PEP as a customer
c) Obtain approval from its senior management before opening an account of a PEP
d) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, obtain the senior management's approval to continue the business relationship
e) Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious

The Company may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for: -

a) PEP, their family members and close associates
b) International Organisation PEP, their family members, and close associates; or
c) PEP who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with the Company present a high risk for money laundering or terrorist financing.

Enhanced Due Diligence (EDD)

Where the risks of money laundering or terrorist financing are high, the Company shall conduct enhanced CDD or Enhanced Due Diligence (EDD) measures, consistent with the risks identified. The EDD measures are as follows: -

a) Obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
b) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the customer or, if applicable, of the Beneficial Owner.
c) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
d) Obtaining the approval of Senior Management to commence or continue the business relationship.
e) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and
f) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Where applicable, it is required that first payment made by a customer in order to open an account with the Company shall be carried out through a bank account in the customer's name with:

a) a Bank
b) a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or
c) subsidiary of a regulated financial institution referred to in b) if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.

For establishing an account-based relationship with high-risk customers, the approval may be given by senior management of the Company or committee of senior managers or an individual member who has been authorised by the senior management in this behalf.

Simplified Customer Due Diligence

Where risk of money laundering or terrorist financing are low, the Company may conduct simplified CDD measures, which should be commensurate with the low risk factors. Examples of possible measures are:

a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship in the manner allowed under the Guidelines;

b) Reducing the frequency of customer identification updates;

c) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold;

d) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

It is hereby clarified that the Company shall not conduct Simplified Due Diligence where there is any suspicion of money laundering or terrorist financing.

Ongoing Due Diligence

a) The Company shall conduct ongoing due diligence on the business relationship with the customer and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Company's knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.

b) For undertaking such ongoing due diligence, the Company shall comply with the following measures:

- ✓ during the course of business relations with a customer, the Company shall observe the conduct of the customer's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with the Company's knowledge of the customer, its business and risk profile and where appropriate, may seek the source of wealth and source of funds;
- ✓ the Company shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose;
- ✓ the Company shall make further enquiries into the background and purpose of the transaction specified in point e) above and document its findings so that this information is made available to the relevant authorities, should the need arise;
- ✓ the Company shall periodically review each customer to ensure that the risk rating assigned to them by the Company in accordance with this policy or the Guidelines commensurate with the money laundering or terrorist financing risk posed by the customer.
- ✓ Where there are indications that the risks associated with an existing business relation with the customer may have increased, the Company shall request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary; and
- ✓ The Company shall ensure that the CDD data documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing CDD data documents and information, particularly for customers with high-risk rating.

7. CUSTOMER ACCEPTANCE POLICY (CAP)

The Company shall ensure compliance with the Customer Acceptance Policy (CAP) adopted by it. The CAP of the Company is given below:

The Company shall ensure that –

a) No account is opened in anonymous or fictitious/ benami name(s).
b) No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
c) No transaction or account-based relationship is undertaken without following the CDD procedure set out in this Policy.
d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is specified.
e) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.
f) it shall apply the CDD procedure at the Unique Customer Identification Code level. Thus, if an existing KYC compliant customer of the Company or with any other entity in the Company's group desires to open another account with the Company, there shall be no need for a fresh CDD exercise.
g) CDD Procedure is followed for all the joint account holders, while opening a joint account.
h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
i) Suitable checks are employed to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by United Nations Security Council (UNSC) or UAPA Order issued by Ministry of Home Affairs (MHA).

301B In Brigade International Financial Centre, 3rd Floor, Building No. 14A, Block-14, Zone 1 Gift City
Gandhinagar GIFT SEZ, Dist. Gandhinagar – 382050, Gujarat, India

j) it does not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non - cooperation of the customer or non-reliability of the data/information furnished to the Company. It shall be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

k) The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

l) The Company shall not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the Company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

8. PERIODIC UPDATION

The Company shall adopt a risk-based approach for periodic updation of CDD. The periodicity of updation from the date of opening of the account / last CDD updation for different categories of customers is as follows:

- ✓ Annually- for high-risk customers
- ✓ Once in three years- for medium risk customer
- ✓ Once in every five years- for low-risk customers

(a) Individual Customers:

(I) No change in CDD information:
In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with the Company or through digital channels (such as online banking / internet banking, e-mail or mobile application of the Company).

(ii) Change in address:
In case of a change only in the address details of the customer, a self-declaration of the new address may be obtained from the customers through e-mail ID registered with the Company or through digital channels (such as online banking / internet banking, e-mail or mobile application of the Company). Further, the Company shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address (in case of change of address only) declared by the customer at the time of periodic updation.

(b) Customers other than Natural Persons:

(i) No change in CDD information:
In case of no change in the CDD information of a customer, which is a non-natural person, a self-declaration through email id registered with the Company, digital channels (such as online banking / internet banking, mobile application of the Company), a letter duly signed by authorised official and requisite resolutions in this regard shall be obtained from the customer. Further, the Company shall ensure that Beneficial Ownership (BO) information available with them is accurate and up to date.

(ii) Change in CDD information:
In case of change in CDD information, the Company shall undertake fresh CDD process as is applicable for on boarding a new customer which is a non-natural person.

In addition to the foregoing, the Company may undertake such additional measures to ensure updation on CDD information as may be prescribed in the Guidelines.

The Company shall ensure that its internal processes on updation / periodic updation of CDD are transparent and adverse actions against the customers are avoided unless warranted by specific regulatory requirements.

9. MONITORING OF TRANSACTIONS

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company may prescribe threshold limits for particular client (s) and pay particular attention to the transactions which exceed these limits.

There shall be periodic review of risk categorization of accounts at least annually. The nature and extent of due diligence will depend on the risk perceived by the Company.

The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, and the source of funds.

10. SANCTION SCREENING

The Company shall review its customers, their business and transactions against United Nations Security Council sanctions lists and also against any other relevant sanctions list which are as under:

a) The "ISIL (Da'esh) & Al-Qaida Sanctions List" which includes name of individuals and entities associated with the Al-Qaida.

b) The "1988 Sanction List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with Taliban
c) OFAC's sanction list

The Company shall also screen its customers against UAPA order issued by MHA (Ministry of Home Affairs).

Further, in addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

The Company shall ensure that details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND and/or the MHA.

The Company shall adhere to the countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government

11. RECORD MANAGEMENT

The Company shall maintain the following records:

a copy of all documents and information obtained in undertaking initial and ongoing CDD of customers;

records of customer business relationships), which include:
correspondence of business and other information relating to a customer's account;
adequate records of transactions to enable standalone transactions to be reconstructed; and
internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a suspicious transaction report.

Notices sent to the Principal Officer of the Company by its employees on suspicious transactions (if any);

All suspicious transaction reports and any relevant supporting documents and information, including internal findings and analysis;

any relevant communications, if made with the FIU-Ind;

Risk assessment documents; and

The records as required by the Act and the Rules.

In addition to the foregoing, the Company shall ensure to preserve the said records in an electronic retrieval form for a minimum of 10 (ten) years from the date on which business relationship has ended or transaction is completed, or such other timeline as may be prescribed under applicable laws.

Risk Assessment Documents

The Company shall keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including: -

a) the business risk assessment undertaken by them as per paragraph 7 of this Policy;
b) how the business risk assessment in (a) above was used for the purposes of risk assessment of customer;
c) the risk assessment of its customer; and
d) the determination of risk rating

Storage of Records

The Company shall ensure that the above records (*if kept in electronic form*) are readily accessible and promptly made available to the Authority or other law enforcement agency, on demand.

The Company may keep above records outside the IFSC, subject to:

(a) take all reasonable steps to ensure that the records are kept in a manner consistent with Guidelines

(b) ensure that the records are easily accessible to it;

(c) ensure that the records are immediately made available for inspection, when so desired by the Authority.

The Company shall evolve a system for proper maintenance and preservation of records in such a manner that allows:

(a) data to be retrieved easily and quickly whenever required or when demanded by the competent authorities;

(b) the Authority or any other competent authority is able to assess the Company's compliance with the applicable laws;

(c) identification of a customer or third party;

(d) it permits reconstruction of any transaction which was processed by or through the Company on behalf of a customer or other third party.

The Company shall verify if there are secrecy or data protection laws that would restrict access without delay to the records referred to herein by the Company or the Authority or the law enforcement agencies of India and where such law exists, the Company shall without delay obtain the copies of the relevant records and keep such copies in a jurisdiction which allows access by the foregoing entities.

12. INTERNAL CONTROL SYSTEM

For the purpose of strengthening of internal control systems, the Company may have independent evaluation of the compliance functions of the Company's policies and procedures. The Company shall further also have an internal audit system to verify compliance with KYC/AML policies and procedures. Auditor's note on status of compliance with the said policy shall be placed before the Board/Audit Committee of the Board.

13. HIRING OF EMPLOYEES AND TRAINING PROGRAMME

The Company shall ensure that it describes KYC norms/AML standards/CFT to its newly hired employees to ensure that criminals not misuse the Company and its business for money laundering or terrorist financing. The Company shall have adequate screening mechanisms in place as an integral part of its personnel recruitment/hiring process.

The Company recognises that it is crucial that all those concerned fully understand the rationale behind this Policy and implement the same consistently. Accordingly, the Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures/AML and CFT mitigation processes of the Company. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers.

The aforesaid training shall enable the Company's employees to:

a) comprehend the applicable laws relating to money laundering and terrorist financing, including the Act and Rules;
b) understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto;
c) recognise and deal with transactions and other activities which may be related to money laundering and terrorist financing;
d) comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;
e) have knowledge of the prevailing techniques, methods and trends in money laundering and terrorist financing, relevant to the business of the Company; and
f) understand their roles and responsibilities in combating money laundering and terrorist financing, including the identity and duties of the Company's Principal Officer and deputy, where applicable.

14. SUSPICIOUS TRANSACTION REPORT (STR)

The Company shall not open an account (or shall consider closing an existing account) when it is unable to apply appropriate CDD measures. In the circumstances when the Company believes that it would no longer be satisfied that it knows the true identity of the account holder, the Company shall also file an STR with FIU-IND. An Indicative List of Suspicious Activities are in Annexure B below.

15. REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA (FIU-INDIA)

Where the Company believes it has come across suspicious activity such as those set out in Annexure B below, the Company shall furnish to the Director, FIU-Ind the required information as set out in the Act and the Rules in the form of an Suspicious Transaction Report (STR).

The STR shall be submitted within 7 days of arriving at conclusion that any transaction or a series of transactions that are integrally connected, are of suspicious nature at the following address in the format prescribed by the FIU-Ind:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Tower-2,
Jeevan Bharati Building,
Connaught Place,
New Delhi-110001

The Company shall not put any restrictions on operations in the accounts where an STR has been made. The Company and its directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND (before, during and after the submission of an STR).

The requirement to report any suspicious transaction applies to all types of transaction. There is no minimum monetary threshold amount for reporting suspicious transactions. Thus, a transaction considered suspicious should be reported to the FIU-IND regardless of the currency or amount of the transaction.

The Company shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. Such records and related documents shall be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. The Company shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

The Company shall make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction.

The Company shall also ensure that Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month, if required.

The Company shall be responsible for timely submission of STR and NTR to FIU-Ind and to ensure confidentiality of STRs in the manner as prescribed in the Guidelines.

16. COMBATING FINANCING OF TERRORISM

Suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The Company, therefore, shall develop suitable mechanism for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-Ind or the Ministry of Home Affairs (MHA) or such other relevant law enforcement authority on priority.

The Company shall before opening any new account, ensure that the name/s of the proposed customer does not appear in the sanction lists set out in paragraph 10 above. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to FIU-Ind or the MHA. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the Company as an integral part of recruitment/hiring process of personnel.

The Company shall take into account risks arising from the deficiencies in AML/CFT regime of FATF black and grey listed countries.

In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the Company shall consider the indicative list of suspicious activities contained in Annexure II below.

17. GENERAL

CUSTOMER EDUCATION

Implementation of KYC procedures require the Company to demand certain information from customers which shall be of personal nature, or which have hitherto never been called for. This may sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company shall educate the customer of the objectives of the KYC, AML and CFT programme. The front desk staffs shall be specially trained to handle such situations while dealing with customers.

APPLICABILITY TO BRANCHES AND SUBSIDIARIES OUTSIDE INDIA

This Policy and the compliance obligations set out in the Act and Rules shall also apply to the Company's branches and majority owned subsidiaries located outside India, if any, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. It is further clarified that in case there is a variance in KYC/AML standards prescribed by the IFSCA and the host country regulators, branches/overseas subsidiaries of the Company shall adopt the more stringent regulation of the two.

Where the law of another jurisdiction does not permit the implementation of KYC/AML-CFT standards that are equivalent to or higher than those that apply to the Company, the Company shall (a) inform the Authority in writing; and (b) apply appropriate additional measures to prevent the ML/TF risks posed by the relevant branch or subsidiary.

The Company may allow for sharing of information between its group companies and including the sharing of information related to CDD and for managing money laundering and terrorist financing risks subject to placing adequate safeguards to protect the confidentiality and use of any information that is exchanged between such group companies.

APPOINTMENT OF COMPLIANCE OFFICER/PRINCIPAL OFFICER/DESIGNATED DIRECTOR

The Company has a senior management officer to be designated as Compliance/Principal Officer ("Officer"). The Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Officer shall maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. In terms of the provisions of the Act and the Rules, the Company shall also designate a person as a 'Designated Director' to ensure overall compliance with the obligations imposed under the PMLA.

18. REVIEW/REVISION OF POLICY

If at any point a conflict of interpretation/information between the Policy and any regulations, rules, guidelines, notification, clarifications, circulars, master circulars/directions issued by relevant authorities ("Regulatory Provisions") arises, then interpretation of the Regulatory Provisions shall prevail.

In case of any amendment(s) and/or clarification(s) to the Regulatory Provisions, the Policy shall stand amended accordingly from the effective date specified as per the Regulatory Provisions. The Board reserve(s) the right to alter, modify, add, delete or amend any of the provisions of the Policy.

Annexure A

Identification of the customers For

individuals

Sr. No.	Particulars	Sr. No.	Particulars
	Full name, including any aliases		Contact details such as personal, office or work telephone numbers
	Unique Identification Number (such as an Identity card number, passport number, etc.)		Occupation or profession, name of employer and location of activity (wherever applicable)
	Date of birth		Information regarding the nature of the business to be conducted; (wherever applicable)
	Nationality		Information regarding the origin of the funds; and (wherever applicable)
	Legal domicile		Information regarding the source of wealth or income. (wherever applicable).
	Current residential address (other than a post office box address)		

For legal person or legal arrangement

In cases where the customer is a legal person or legal arrangement, the Company shall, apart from identifying the customer, shall also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. Additionally, the Company shall also identify and screen the related parties or connected parties of such customer and should remain apprised of any changes to connected parties.

For identification of the connected parties, the Company shall obtain the following information of each related or connected party:
(i) full name, including any aliases; and
(ii) Unique Identification Number (such as an Identity card number, passport number, etc.).

Verification of the customers

For Individuals

Features	Documents
Identity proof (Indian)	Passport
	Driving License
	Proof of possession of Aadhar number
	Voter's Identity Card issued by Election Commission of India
Identity proof (Foreign)	Passport
	Driving License
	National Identity card
	Voter identification card
Address proof (Indian & Foreign)	Utility bill (electricity, telephone, post-paid mobile phone, piped gas, water bill)-not more than 2 months old
	Property, Municipal tax receipt, city council tax receipt, or such other equivalent document
	Bank account or Post Office savings bank account statement or statement of foreign bank (Applicable only in case of low risk)
	Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
	Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.
Note	In case the OVD presented by a foreign national does not contain the details of address, the documents issued by the Government departments of foreign jurisdictions or letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

For legal person or legal arrangement

Features	Documents
Company	Certificate of incorporation
	Memorandum and Articles of association
	PAN or equivalent document prevalent in the home jurisdiction of the Customer
	Board resolution authorising officers or employees, as the case may be, to transact on its behalf
	Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Company

301B In Brigade International Financial Centre, 3rd Floor, Building No. 14A, Block-14, Zone 1 Gift City
Gandhinagar GIFT SEZ, Dist. Gandhinagar – 382050, Gujarat, India

Partnership/Limited Liability Partnership	Registration certificate
	Deed of Partnership
	PAN or equivalent document prevalent in the home jurisdiction of the Customer
	Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Company
Trust	Registration certificate
	Trust Deed
	PAN or equivalent document prevalent in the home jurisdiction of the Customer
	Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Company
Unincorporated Associations/ Bodies	Resolution of the managing body of such association/body
	PAN or equivalent document prevalent in the home jurisdiction of the Customer
	Power of attorney granted to transact on its behalf
	Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Company

The Company may ask to submit such other documents as may be required by the to establish the existence.

ANNEXURE –B

Non exhaustive list of Suspicious Activities:

a) Transactions Involving Large Amounts of Cash Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the Company

b) Transactions that do not make Economic Sense

c) Activities not consistent with the Customer's Business

d) Attempts to avoid Reporting/Record-keeping Requirements:

- ✓ Customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- ✓ Any individual or group that coerces/induces or attempts to coerce/induce a VTI employee not to file any reports or any other forms.
- ✓ An account where there are several cash transactions below a specified threshold level to a avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

e) Unusual Activities - Funds coming from the countries/centres which are known for money laundering.

f) Customer who provides Insufficient or Suspicious Information:

- ✓ A customer/Company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
- ✓ A customer/Company who is reluctant to reveal details about its activities or to provide financial statements.
- ✓ A customer who has no record of past or present employment but makes frequent large transactions.

g) Certain Employees arousing Suspicion:

- ✓ An employee whose lavish lifestyle cannot be supported by his or her salary.
- ✓ Negligence of employees/willful blindness is reported repeatedly.

h) Some examples of suspicious activities/transactions to be monitored by the operating staff:

- ✓ Large volume of Transactions
- ✓ Multiple accounts under the same name
- ✓ Sudden surge in activity level
- ✓ Same funds being moved repeatedly among several accounts

For details, please read International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 available at:
https://ifsca.gov.in/CommonDirect/GetFileView?id=d575554ec59b09e7fde503d3a807d7be&fileName=Master_Guidelines_Feb26_2026_20260227_0352.pdf&TitleName=Legal

301B In Brigade International Financial Centre, 3rd Floor, Building No. 14A, Block-14, Zone 1 Gift City
Gandhinagar GIFT SEZ, Dist. Gandhinagar – 382050, Gujarat, India