BEAMER TRADES AND TECHNOLOGIES (OPC) PVT. LTD.

Volume 1.2

Dated- 24th May 2025

ANTI-MONEY LAUNDERING (AML)

COUNTERING THE FINANCING OF TERRORISM (CFT)

KNOW YOUR CUSTOMER (KYC), CUSTOMER DUE DILIGENCE (CDD)

RISK ASSESSMENT POLICY

In accordance with:

- **The Prevention of Money Laundering Act (PMLA), 2002**
- **RBI Master Direction on KYC (as amended up to May 2023)**
- **SEBI Master Circular on AML-CFT (August 2023)**
- **FIU-IND Reporting Guidelines**

Prepared and raised by:
Chief Compliance Officer- Gaurav Kumar Singh, PO and Compliance Officer
Beamer Trades and Technologies (OPC) Pvt. Ltd.

Approved by:
Board of Directors- Ashish Shukla, CEO and Designated Director
Approval Date: 24th of May 2025 | Mayur Vihar

For BEAMER TRADES AND TECHNOLOGIES (OPC) PVT. LTD. Director

Corporate Office: 101, Pratap Nagar, Mayur Vihar Phase 1,
East Delhi, Delhi, India – 110091
Phone - +917839285187
Email - legal@beamertrades.com
Website- exchange.koinbae.com

Effective from 25th of mar 2028

BEAMER TRADES AND TECHNOLOGIES (OPC) PVT. LTD.

Know Your Customer (KYC), Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) Policy (KYC-AML-CFT Policy)

1. Introduction

This Know Your Customer (KYC), Anti-Money Laundering (AML), and Combating the Financing of Terrorism (CFT) Policy (hereinafter referred to as the "KYC-AML-CFT Policy") is a formal declaration of Beamer Trades and Technologies (OPC) Pvt. Ltd. ("BTTPL" or the "Company") and its unwavering commitment to uphold ethical business practices and global compliance standards. This Policy outlines the principles, framework, and procedures designed to prevent the misuse of BTTPL's platform and services for illicit financial activities, including money laundering, terrorism financing, and other unlawful conduct.

BTTPL is a forward-looking technology-driven company focused on digital financial services, trading platforms, algorithmic strategies, and virtual digital assets service providers (VDASP). In doing so, the Company interacts with diverse users and stakeholders who access its services via online and technology channels. Recognizing the potential risks inherent in digital financial environments, BTTPL has proactively chosen to adopt and implement a comprehensive risk-based KYC and AML compliance program.

Although BTTPL is not currently classified as a "reporting entity" under the provisions of the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, or the Unlawful Activities (Prevention) Act, 1967, the Company has voluntarily adopted this policy in line with international best practices and recent guidance under the AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets, as issued by the Financial Intelligence Unit of India (FIU-IND).

This Policy affirms that the services offered by BTTPL are not to be used, directly or indirectly, for the facilitation of any criminal conduct or financial malpractice. It is designed to ensure that the Company maintains an effective internal control environment capable of:

- Identifying and verifying the identity of users;
- Assessing and categorizing customer risk;
- Monitoring transactions for suspicious activity;
- Escalating red flags and filing suspicious transaction reports where appropriate;
- Ensuring appropriate governance and audit trails of compliance efforts.

Through this document, BTTPL seeks to:

- Reinforce its business integrity and promote a compliance culture;
- Build confidence among customers, regulators, and stakeholders;
- Align its internal procedures with the emerging regulatory expectations, especially in digital finance and VDA environments;
- Prevent the exploitation of its platform and services for money laundering, terrorism financing, or other illicit purposes.

In this context, the Company acknowledges and aligns its practices, voluntarily and in spirit, with the following key legal and regulatory frameworks:

- Prevention of Money Laundering Act, 2002 (as amended);
- Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (as amended);
- Unlawful Activities (Prevention) Act, 1967;
- AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (FIU-IND, March 2023);
- Any relevant circulars, advisories, or enforcement trends emerging from national or global AML regulators.

The Company shall maintain internal policies, controls, and procedures that are subject to periodic review and updates, in response to legal changes, operational needs, and evolving typologies of financial crime.

2. Scope

This KYC-AML-CFT Policy applies comprehensively to all users, customers, business partners, and associated persons engaging with Beamer Trades and Technologies (OPC) Pvt. Ltd. (BTTPL), including through its

online platforms, specifically the website exchange.koinbae.com, related mobile applications, software tools, APIs, or any other digital or physical services, whether current or introduced in the future (collectively referred to as "Online Platforms").

All Users must carefully read, understand, and explicitly accept the terms of this Policy before using or accessing any BTTPL services. By continuing to browse, transact on, or otherwise engage with BTTPL's Online Platforms, Users agree to be contractually bound by the provisions of this KYC-AML-CFT Policy. Failure to comply with or consent to these terms shall result in an immediate prohibition against accessing or using BTTPL's services.

The terms "We", "Our", "Us", and "Company" refer to Beamer Trades and Technologies (OPC) Pvt. Ltd., including its owners, directors, shareholders, employees, contractors, affiliates, and service providers. The terms "You", "Your", or "User" refer to any person or legal entity accessing or using BTTPL's Online Platforms.

This Policy applies to all products, services, and transactions offered by BTTPL and requires all users and customers to adhere strictly to the identity verification and ongoing monitoring measures set out herein. The identity verification process includes, but is not limited to, the submission of valid government-issued documentation such as PAN cards, proof of address, and any other documents deemed necessary under applicable law or the Company's internal risk policy.

This Policy is a binding part of BTTPL's User Terms and Conditions and is designed to prevent the misuse of its services for money laundering, terrorist financing, fraudulent transactions, or any other illegal or unethical activities. The Company reserves the right to continuously monitor all user activity on the Online Platforms and collect, analyze, or report information as required for the purpose of maintaining compliance with this Policy.

BTTPL further reserves the unilateral right to modify, revise, or replace any part of this Policy at its sole discretion without prior notice. Users are

solely responsible for reviewing the Policy periodically and maintaining compliance with any changes.

This Policy shall also be read in conjunction with BTTPL's Terms of Use and Privacy Policy, and together these documents form a unified framework governing user interaction, risk management, and lawful usage of the Company's services.

Scope — Key Points

- Applies to all BTTPL services, including the exchange.koinbae.com website, mobile apps, and related future platforms.
- Binding on all Users, regardless of their geographic location, user status, or method of access.
- Applies equally to all BTTPL employees, consultants, contractors, and partners.
- Users must read, understand, and expressly agree to this Policy before accessing or using BTTPL services.
- Users must comply with the identity verification process, including submission of official KYC documents like PAN cards and proof of address.
- Continuous monitoring of user activity is a core part of the Policy's enforcement, and Users consent to such monitoring by using the services.
- Violations of this Policy may result in account suspension, termination, or reporting to appropriate regulatory authorities.
- The Policy is subject to unilateral modification by BTTPL, and Users are responsible for keeping themselves updated.
- The Policy must be read along with the User Terms and Conditions and Privacy Policy, which together govern the contractual relationship between BTTPL and the User.

3. Objectives

The objective of this KYC-AML-CFT Policy is to define clear, enforceable standards for customer verification, risk management, and transaction monitoring that prevent the misuse of BTTPL's services for money laundering, terrorist financing, and other unlawful activities. The Policy

ensures that all Users of the BTTPL Online Platforms — whether individual or corporate — undergo a structured and risk-based identification process before availing of any services. By mandating this, the Company not only complies with ethical and legal expectations but also secures its business operations against regulatory, financial, and reputational risks.

BTTPL is committed to remaining vigilant in its fight against financial crimes and, in its best judgment, implements monitoring processes and controls to prevent any individual or entity from using its services to facilitate money laundering, terrorist financing, or any other illicit conduct. The Policy also seeks to educate and obligate Users to act responsibly, ethically, and in strict compliance with applicable laws. This Policy enshrines BTTPL's philosophy of proactive prevention, ongoing surveillance, timely reporting, and continuous refinement of its risk control measures. Additionally, the Company's contractual and legal relationship with Users is defined by their express acceptance of this Policy as part of the User onboarding process.

This document also acts as a statement of commitment from BTTPL to adhere to the evolving legal landscape, including updates to the Prevention of Money Laundering Act, 2002, the AML & CFT Guidelines for Virtual Digital Asset Service Providers issued by FIU-IND, and emerging standards laid down by national and international regulatory bodies.

Objectives — Key Points

- Prevent the misuse of BTTPL's Online Platforms and services for money laundering, terrorist financing, and other illicit purposes.
- Mandate the collection, verification, and validation of customer identification data, including PAN cards, proof of address, and other legally prescribed documentation.
- Ensure that Users agree to this Policy before engaging in any transaction or accessing BTTPL services.
- Enforce a risk-based customer classification system and apply Enhanced Due Diligence (EDD) for high-risk Users.
- Enable continuous monitoring of all User transactions and behavioral patterns for suspicious activities.

- Promote an ethical culture by obligating both Users and employees to detect and prevent financial crimes.
- Establish clear escalation procedures for suspicious transactions to be reported to the Financial Intelligence Unit of India (FIU-IND).
- Ensure full transparency in customer engagement and maintain strict data security and confidentiality.
- Empower BTTPL to update the Policy periodically, with continued use of the services implying User acceptance of all modifications.
- Uphold compliance with the Terms of Use, Privacy Policy, and applicable laws, reinforcing the Company's anti-financial-crime ecosystem.

4. Definitions

4.1. "Applicable Law" shall mean any applicable statute, law, regulation, ordinance, rule, judgment, order, decree, by-law, approval from the concerned authority, government resolution, order, directive, guideline, policy, requirement, or other governmental restriction in force in India, including without limitation the Foreign Exchange and Management Act, 1999 and regulations thereunder, Prevention of Money Laundering Act 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules 2005 ("PMLR"), AML & CFT Guidelines For Reporting Entities Providing Services Related To Virtual Digital Assets ("AML Guidelines"), as issued by the Financial Intelligence Unit – India ("FIU-IND"), and various applicable guidelines, rules and regulations of the Computer Emergency Response Team, India ("CERT-In"), replaced and updated from time to time;

4.2. "Designated Director" means a person designated by BTTPL to ensure overall implementation of the obligations imposed under chapter IV of the PMLA and the PMLR;

4.3. "Principal Officer" means an officer designated by BTTPL to ensure compliance with the obligations imposed under chapter IV of the PMLA and the PMLR;

4.4. "Crypto(s)" are Virtual Digital Assets ("VDA") and refer to a cryptographically secured digital representation of value or contractual

rights that uses distributed ledger technology and can be transferred, stored or traded electronically using the Platform, including but not limited to bitcoin and ether;

4.5. "Customer"/ "User" shall mean any Person using/accessing the Platform or interacting with it in any manner for buying, selling, depositing or withdrawing Crypto(s);

4.6. "Customer Due Diligence" (CDD) means identifying the Customer and verifying their identity by using a reliable, independent source of documents, data, or information, and checking if there are any sanctions or adverse media matches against them;

4.7. "Officially Valid Document" (OVD) means the Passport, the Driving License, proof of possession of an Aadhaar Number, or the Voter's Identity Card issued by the Election Commission of India. For the purpose of this definition, 'Aadhaar Number' means an identification number as defined under the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

4.8. "Person" means an individual who is above eighteen (18) years of age and an Indian citizen.

4.9. "Organization" means any entity registered in India that carries out the function of a business and has a separate legal existence from the individuals associated with it.

4.10. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. A User could also qualify as a PEP if the User is a family member or a close relative of such an individual.

4.11. "Virtual Digital Assets" (VDA) means any information or code or number or token (not being Indian or foreign currency), a non-fungible token or any digital asset as defined under Section 2(47A) of the Income Tax Act, 1961.

4.12. "Permanent Account Number" (PAN) is issued by the Indian Income Tax Department to help uniquely identify taxpayers. e-PAN is an electronically issued PAN which is digitally signed.

4.13. "Beneficial Owner" means the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted, and includes any person who exercises ultimate effective control over a juridical person.

4.14. "Suspicious Transaction" means a transaction, attempted transaction, or series of transactions, whether cash or non-cash, which to a reasonable person, appears unusual, lacks economic or lawful purpose, or involves funds derived from illegal activities or intended to be used for illegal purposes, or is designed to evade regulatory reporting requirements.

4.15. "Enhanced Due Diligence" (EDD) means additional procedures, investigations, and monitoring applied to higher-risk categories of Customers, including but not limited to Politically Exposed Persons (PEPs), customers from high-risk jurisdictions, and transactions or relationships that exhibit higher-than-normal money laundering or terrorism financing risks.

4.16. "Risk-Based Approach" (RBA) refers to a methodology where the Company assesses and categorizes its customers, products, services, delivery channels, and geographic locations to apply proportionate levels of Customer Due Diligence, monitoring, and controls commensurate with the identified risk.

4.17. "Sanctions List" means the list of individuals, entities, and countries maintained and published by regulatory or governmental authorities including, but not limited to, the Reserve Bank of India (RBI), the Financial Intelligence Unit-India (FIU-IND), the United Nations Security Council (UNSC), the Office of Foreign Assets Control (OFAC), or any other competent authority, which the Company is obligated to review before onboarding or continuing a relationship with a Customer.

4.18. "Transaction Monitoring" refers to the automated or manual process of reviewing customer transactions on an ongoing basis to identify patterns or individual instances of suspicious activity that could indicate a potential violation of law or Company policy.

4.19. "Wallet Address" means a unique alphanumeric identifier that represents a destination on a blockchain network for sending and receiving Virtual Digital Assets.

5. Customer Acceptance Policy ("CAP")

Our services are exclusively offered to individuals holding Indian citizenship and residing within India. The designation of "User" applies only to those who meet these criteria.

Residency is defined as having a valid, permanent or habitual residential address in India, supported by official documentation. Accessing the Platform using proxy servers, VPNs, or from foreign jurisdictions is strictly prohibited, and any such attempt may result in immediate account suspension and compliance review.

All Users must read, understand, and agree to this KYC-AML-CFT Policy prior to accessing BTTPL services. Use of the Platform implies express acceptance of this Policy.

5.1.1 Know Your Customer (KYC) is an essential regulatory and operational standard for BTTPL. It ensures that all Users are properly identified and verified before being allowed access to the Platform. KYC is performed not only to comply with legal obligations under the PMLA, PMLR, and AML Guidelines, but also to enforce safe platform usage in line with the directions under the Information Technology Act, 2000 (CERT-In advisory dated April 28, 2022).

Objectives of KYC:

a) Ensure accurate Customer identification.
b) Monitor transactional behavior for suspicious patterns.
c) Prevent association with insolvent or legally disqualified individuals.
d) Minimize fraud and identity theft.
e) Avoid dealing with anonymous or fictitious Users.
f) Ensure that only reliable and legitimate Users are onboarded.

BTTPL verifies submitted documentation and maintains audit trails for every KYC submission, update, and modification.

5.1.2 Safeguard Measures by BTTPL

Before granting access to the Platform:

- Users must not use fictitious identities.
- Customer Due Diligence (CDD) must be completed successfully.
- Non-cooperative Users or Users providing unverifiable or unreliable documents will be denied access.
- All transactions require completion of the CDD process before execution.

Users are strictly prohibited from acting on behalf of others, using third-party funds, or disguising beneficial ownership. Users must act solely for their benefit.

BTTPL retains the right to:

- Review the User documentation at any time.
- Suspend, freeze, block, or terminate any User account based on internal reviews or external law enforcement requests.
- Refuse access to new Users or discontinue access to existing Users when compliance conditions are not satisfied.

BTTPL also screens all Users against Sanctions Lists, including those published by the UN Security Council, OFAC, and FIU-IND.

5.2.1Know Your Business (KYB) Policy

In addition to identifying and verifying individual Users, BTTPL recognizes the importance of conducting due diligence on all institutional and entity-based customers to mitigate the risks of money laundering, fraud, terrorist financing, or other unlawful activities. This process is referred to as Know Your Business (KYB).

5.2.2 BTTPL applies KYB verification to all legal entities, including but not limited to:

- Private Limited Companies,
- Partnerships,
- Limited Liability Partnerships (LLPs),

- Trusts,
- Foundations,
- Societies,
- Non-profit organizations (NPOs).

5.2.3 The KYB process involves:

a) Verification of the entity's legal existence through appropriate corporate documentation, including:

- Certificate of Incorporation or Registration,
- Memorandum and Articles of Association / Partnership Deed,
- GST Registration, if applicable,
- Proof of registered office address,
- PAN or TAN.

b) Verification of **ownership structure** to identify:

- Directors, Partners, or Trustees,
- Ultimate Beneficial Owners (UBOs) as defined by PMLA.

c) Screening of the entity, its directors, and UBOs against:

- Sanctions Lists (UNSC, OFAC, EU, FIU-IND),
- Adverse media coverage,
- Regulatory blacklists.

d) Assessment of the entity's business model, anticipated transaction volumes, and source of funds to ensure alignment with the nature and purpose of the intended relationship.

5.2.4 Entities must promptly notify BTTPL of any changes to their:

- Ownership,
- Control,
- Business structure,
- Authorized signatories,
- Registered address.

5.2.5 KYB verification is a prerequisite for account activation and is subject to Periodic Review at intervals based on the customer's risk classification, or as triggered by a material change or suspicion.

6. Customer Identification Procedure ("CIP")

The purpose of the Customer Identification Procedure (CIP) is to establish the User's true identity at the time of onboarding and throughout the business relationship, in accordance with the Prevention of Money Laundering Act, 2002 (PMLA), FIU-IND Guidelines, and FATF Recommendations.

The CIP is applicable during:

- Customer onboarding (individuals, corporates, trusts, etc.)
- Transaction initiation or significant activity change
- Periodic KYC reviews based on risk category
- Trigger events (e.g., change in control, address, UBO, unusual transaction)

6.1 Customer Identification & Verification – Individuals

The BTTPL must ensure the following steps are followed for all individual customers:

A. Mandatory Information Collected:

- Full name (as per Officially Valid Document)
- Date of birth and gender
- Residential and mailing address
- Nationality and citizenship
- Email and mobile number

- Purpose and nature of the business relationship
- Occupation/employment details

B. Documents Required (as per OVD definition):

- PAN Card (mandatory for financial transactions)
- Any one of the following:
    - Aadhaar (Offline/Masked)
    - Passport
    - Driving License
    - Voter ID
- Proof of address (utility bill, bank statement – not older than 3 months)

C. Enhanced Verification Tools:

- Selfie and liveness detection using biometric tools
- Geolocation verification (IP/device tracking)
- Mobile and email OTP validation
- Bank account ownership verification

6.2 Customer Identification – Non-Individual Customers

For legal entities and non-person entities, the BTTPL must collect and verify:

A. Business Information Required:

- Legal name of the entity
- Country of incorporation and business license
- Registered business address
- Nature of business and expected transaction volume

- Tax Identification Number / PAN
- Names and positions of all directors and senior management

B. Mandatory Documents:

- Certificate of Incorporation/Registration
- Memorandum & Articles of Association
- Board Resolution authorizing account opening
- PAN of the entity
- List of directors and authorized signatories
- UBO Declaration
- Recent proof of business address

6.3 Ultimate Beneficial Owner (UBO) Identification

A. UBO Definition (as per PMLA Rules):

A UBO is any natural person who owns or controls 10% or more of an entity or has controlling interest through other means.

B. Information & Documents:

- Full name, DOB, nationality, and country of residence
- Ownership percentage or control basis
- Source of wealth/funds
- Self-attested identity & address documents
- Signed UBO Declaration Form

C. Verification Requirements:

- Sanctions & PEP list screening
- Adverse media checks

- In-person or video KYC (if required)

6.4 Video KYC

Video-based customer identification shall be carried out where:

- Automated verification fails
- Required under Enhanced Due Diligence
- Triggered by suspicious transaction or risk indicators

BTTPL shall ensure secure, recorded sessions with location stamping and biometric confirmation.

6.5 Customer Due Diligence (CDD) & Risk-Based Approach

BTTPL categorizes customers into Low, Medium, and High risk. The BTTPL shall ensure:

Risk Level	Requirements
Low	Basic KYC, limited transaction monitoring
Medium	ID verification + ongoing monitoring
High	EDD: SOW/SOF, in-person/video verification, frequent review

Risk classification is based on: transaction size, country risk, customer profile, type of asset, involvement of intermediaries.

6.6 Ongoing Monitoring and Trigger Events

The BTTPL must ensure continued review of:

- Transactions inconsistent with declared profile
- Suspicious behavior
- Cross-border or privacy-enhancing VDA transactions
- Any mismatch in identity data or fraud risk

- Triggers: Address change, ownership change, large new transactions

6.7 KYC Renewal Frequency

Risk Level Review Period

Low Annually

Medium Annually

High Annually

Changes in any information must be updated promptly, and new documents must be collected when validity expires. Screening Obligations

BTTPL must ensure:

- Real-time screening against OFAC, UN, EU, and RBI sanctions lists
- PEP identification and escalation for EDD
- Use of AI tools for adverse media tracking
- Wallet address risk scoring (blockchain analytics)
- Risky Geolocation check ins

6.7 Record Keeping

- All CIP/KYC data must be retained for at least 5 years after termination of the business relationship.
- Video recordings (if applicable) must be securely stored and made available upon request by authorities.
- All STR filings, decision logs, and verification records must be logged by the BTTPL.

6.8 Compliance, Oversight & Training

The BTTPL shall:

- Ensure all compliance obligations are met under PMLA and FIU-IND directions

- Conduct quarterly compliance checks and self-audits
- Undergo annual AML/KYC training
- Maintain a log of escalations and suspicious findings

6.9 Review and Amendments

This CIP shall be reviewed at least annually or earlier if required by:

- Updates in PMLA or FIU-IND guidelines
- Technology/process enhancements
- Regulatory examination feedback

Changes must be approved by the Designated Director and communicated to all impacted teams.

7. Anti-Money Laundering (AML) Standards

As an aspiring registered Reporting Entity (RE) with the Financial Intelligence Unit - India (FIU-IND), BTTPL has implemented a robust AML framework that:

- Ensures strict compliance with the PMLA, PMLR, and AML Guidelines for VDA Service Providers.
- Identifies and blocks customers involved in or suspected of money laundering, terrorism financing, or other prohibited activities.
- Screens all Users and counterparties against national and international watchlists.

7.1 Measures to Prevent Money Laundering & Terrorist Financing

BTTPL implements proactive measures to prevent misuse of its services, including:

- Continuous transaction monitoring.
- Sanctions screening.
- Source-of-funds verification.
- Real-time risk-based alerts and compliance intervention.

8. Monitoring of Transactions – Ongoing Due Diligence

Beamer Trades and Technologies (OPC) Pvt. Ltd. ("BTTPL") is committed to implementing robust monitoring mechanisms to detect, deter, and report suspicious activities throughout the life cycle of a customer relationship. Ongoing Due Diligence (ODD) is a core component of BTTPL's risk-based approach under the **Prevention of Money Laundering Act, 2002 (PMLA)** and the **AML & CFT Guidelines** issued by **FIU-IND**.

Ongoing monitoring applies to:

- All transactions executed or attempted through BTTPL's platform;
- Behavioral patterns that deviate from the customer's known profile;
- Deposits, withdrawals, and wallet interactions involving Virtual Digital Assets (VDAs);
- Activity involving high-risk jurisdictions or flagged wallet addresses.

BTTPL uses a combination of automated transaction monitoring systems (TMS) and manual oversight to identify:

- Unusual or large-value transactions inconsistent with customer's profile;
- Rapid movements of VDAs between multiple wallets (layering);
- Multiple accounts being operated from the same device/IP address;
- Use of mixers, tumblers, or privacy coins;
- Transactions involving blacklisted or flagged wallet addresses;
- Cross-border transfers involving high-risk or non-cooperative jurisdictions.

8.1 Prohibited Activities

The following activities are strictly prohibited on the BTTPL platform. No User shall, directly or indirectly, engage in or facilitate any of the following activities:

i) Fraud: Any intentional deception made for personal gain or to damage another individual or entity, including misrepresentation of identity, financial status, or source of funds.

ii) Corruption: Offering, soliciting, or accepting bribes or undue advantages to influence a transaction or decision related to the use of BTTPL's services.

iii) Collusion: Any arrangement or conspiracy between two or more parties to defraud or mislead BTTPL or its users.

iv) Terrorist Financing: Providing, collecting, or moving funds with the knowledge or intent that such funds may be used, in full or in part, to support terrorist acts or organizations.

v) Criminal Conduct: Any action that constitutes an offence under applicable Indian law or any international legal framework to which India is a party.

vi) Money Laundering: As defined under Section 3 of the Prevention of Money Laundering Act, 2002 — including concealment, possession, acquisition, or use of proceeds of crime and projecting it as untainted property.

8.2 Enforcement and Action by BTTPL

If BTTPL, through internal detection mechanisms, partner systems, or alerts from regulatory/law enforcement agencies, suspects that a User is involved in any of the above prohibited activities, the following actions may be immediately initiated:

8.2.1 Account Suspension

- The User's account will be temporarily suspended to prevent further transactions pending investigation.
- Withdrawal and deposit functions will be frozen to mitigate the risk of asset flight.

8.2.2 Investigation and Escalation

- A formal internal investigation will be launched by BTTPL's Compliance and Risk Team.
- BTTPL will perform Enhanced Due Diligence (EDD) including source of funds verification, transaction history analysis, and identity re-validation.
- The matter will be escalated to the Designated Director and Principal Officer for decision-making and regulatory coordination.

8.2.3 Reporting to Authorities

- If the activity meets the threshold of suspicion under the PMLA or AML Guidelines, a Suspicious Transaction Report (STR) shall be filed with the Financial Intelligence Unit – India (FIU-IND) within seven working days of internal escalation.
- In serious cases (e.g. suspected terrorist financing or large-scale fraud), BTTPL may also report the matter directly to:
    - Cybercrime division of local/state police
    - Directorate of Enforcement (ED)
    - CERT-In, if it involves a cyber threat component

8.2.4 Termination and Blacklisting

- Upon confirmation or strong suspicion of prohibited activity, BTTPL may:
    - Permanently terminate the User's access to its platform,
    - Add the individual/entity to an internal blacklist,
    - Share the User's KYC and transaction trail with law enforcement, as required under law.

8.2.5 Legal Cooperation

- BTTPL shall cooperate fully with law enforcement and regulatory authorities by providing transaction logs, IP access history, KYC documents, and any other relevant information, subject to applicable privacy laws.

- If assets are linked to criminal conduct, BTTPL may initiate or support asset freezing, as permitted under Indian law or by court order.

8.2.6 Communication with Affected Parties

- Affected users (e.g. recipients of fraudulent transactions) may be notified if necessary to protect them from further harm or loss.
- However, BTTPL may delay such communication if it is advised to do so by regulatory or law enforcement authorities.

8.3 Know Your Transaction (KYT) Policy BTTPL implements Know Your Transaction (KYT) protocols to monitor and assess the consistency, legitimacy, and risk associated with every transaction initiated, attempted, or completed through its Platform.

8.3.1 The KYT process involves:

a) Analyzing transaction behavior in relation to the User's:

- Historical patterns,
- Known risk profile,
- Declared source of funds,
- Nature of business or personal financial circumstances.

b) Identification and automated flagging of:

- High-value transactions exceeding internal risk thresholds,
- Multiple rapid transactions inconsistent with known patterns,
- Transactions linked to high-risk jurisdictions or blacklisted wallet addresses,
- Wallet addresses flagged in known cybercrime, money laundering, or terrorism financing databases.

8.3.2 All flagged transactions will be subject to:

- Manual review by the Compliance Team,
- Potential suspension pending further verification,
- Reporting to regulatory authorities via STR, if found suspicious.

8.3.3 KYT is applied not only to completed transactions but also to:

- Transaction attempts,
- Deposits or withdrawals awaiting confirmation,
- Incoming or outgoing VDA flows.

8.3.4 The KYT Framework operates in tandem with the Company's transaction monitoring systems and forms a key component of its AML-CFT controls, ensuring both proactive detection and regulatory compliance.

Note: - Travel Rule Compliance is explained later in the policy at section 10.

9. Risk Management Framework

The objective of BTTPL's Risk Management Framework is to ensure that all customers are onboarded, monitored, and reviewed in accordance with their risk profile. BTTPL classifies all customers into three distinct risk categories based on their profile, behavior, and exposure level. This classification determines the level of due diligence, transaction monitoring, and frequency of KYC updates.

A. Low-Risk Customers

These customers typically present minimal AML/CFT risks. Characteristics include:

- Fully verified identity and address through Officially Valid Documents (OVDs).
- Limited or infrequent transactions.
- Individuals with transparent financial activities and no adverse media alerts.
- No links to high-risk jurisdictions or politically exposed persons (PEPs).

Examples:

- Salaried individuals with consistent transaction behavior.
- Verified retail investors with nominal trading volume.

- Senior citizens or students using the platform occasionally.

Controls Applied:

- Basic Due Diligence (BDD).
- KYC renewal on an annual basis.
- Standard transaction monitoring.

B. Medium-Risk Customers

These customers require a moderate level of scrutiny due to the nature of their profession or activity level.

Examples:

- Freelancers or self-employed individuals with varying income streams.
- Small business operators or consultants handling moderate transaction volumes.
- Individuals with minor discrepancies in initial KYC that are resolved during onboarding.

Risk Indicators:

- Spikes in transaction volumes.
- Infrequent inconsistencies in wallet use.
- Transactions with counterparties in low-transparency jurisdictions.

Controls Applied:

- Full CDD.
- Sanctions screening at onboarding and quarterly.
- KYC renewal on an annual basis.
- Behavioral monitoring using system alerts.

C. High-Risk Customers

Customers falling into this category present an elevated AML/CFT risk and are subject to Enhanced Due Diligence (EDD).

Examples:

- Politically Exposed Persons (PEPs) and their close associates.
- Customers with significant activity from or ties to FATF-designated high-risk jurisdictions (e.g., North Korea, Iran).
- Users with complex financial arrangements or frequent use of privacy-enhancing technologies (mixers, tumblers).
- Individuals or entities with adverse media exposure or past regulatory violations.
- Risky Geo belongings.
- NRIs with history tied to weak AML countries.
- Less Skilled , Less Qualified individuals

Controls Applied:

- EDD at onboarding and periodic review.
- Source of funds and source of wealth documentation.
- Frequent sanctions re-screening (monthly or real-time).
- KYC renewal on an annual basis.
- Approval by Compliance Officer or Principal Officer required before onboarding.

Risk categorization is determined by:

- Customer background.
- Place of residence.
- Occupation or nature of business.
- Transaction patterns.
- Watchlist and sanctions screening.

9.1 Risk Reassessment & Trigger Events
Risk profiles are reviewed:

- **High Risk:** Every 12 months.
- **Medium Risk:** Every 12 months.
- **Low Risk:** Every 12 months.

Trigger-based reviews occur when:

- Suspicious activity is detected.

- Law enforcement or regulators raise an alert.
- Negative news or sanctions list hits the User.

9.2 Customer Onboarding Exclusions
BTTPL will refuse onboarding if:

- The customer is flagged for money laundering or terrorist financing.
- The customer is associated with blacklisted or high-risk countries.
- The customer is linked to illegal business operations.
- The customer is a PEP with ties to high-risk jurisdictions.

10. Record-Keeping & Data Retention

10.1 All KYC data, CDD records, transaction logs, and risk assessments are:

- Retained for at least **5 years** from the date of account closure or transaction completion.
- Retained beyond 5 years if required by regulators or enforcement agencies.
- Subject to confidentiality and secure storage protocols.

11. Declarations and Obligations

11.1 Declarations and Disclosure of Information by BTTPL

11.1.1 BTTPL shall identify and verify the identity of each User at the time of onboarding, before permitting any trading, deposits, withdrawals, or other financial transactions via the Platform. Verification may involve requesting specific documents and data and leveraging third-party tools, software, or technology partners for identity verification and validation of User-provided information.

11.1.2 All documents and data collected during KYC, Customer Identification, or ongoing due diligence shall be accessed, processed, and retained by BTTPL strictly under this Policy, the Privacy Policy, and Applicable Laws.

11.1.3 BTTPL shall verify User identity through 'Surepass' and 'Signzy' which are reliable and lawful sources, which may include, but are not limited to:

a) PAN / e-PAN verification via government-approved systems;
b) Aadhaar (Masked/Offline) or Proof of Possession under the Aadhaar Act, 2016;
c) Passport verification under the Passports Act, 1967;
d) Voter ID verification under the Election Commission of India;
e) Any other document or identifier as may be required by BTTPL from time to time for compliance or risk management purposes.

In addition to document-based verification, BTTPL reserves the right to employ **Sanctions List Screening** (e.g., UNSC, OFAC, FIU-IND) to confirm that the User is not listed on any domestic or international restricted lists.

11.1.4 Failure by the User to provide the requested documents, identity information, or cooperation for regulatory verification processes shall result in the suspension or restriction of access to the Platform and may lead to the withholding of deposits, blocking of withdrawals, or termination of User services.

This also applies in situations where **Travel Rule** data is missing, incomplete, or non-verifiable.

11.1.5 The list of acceptable documents and verification criteria may be updated by BTTPL at its sole discretion, and such updates shall be binding on Users without prior notice.

11.1.6 BTTPL reserves the right to seek further documentation or information at any time for:

a) Verifying the User's financial status or source of funds;
b) Confirming the ownership of any Crypto wallet involved in deposits or withdrawals;
c) Establishing the legitimate origin and intended use of Virtual Digital Assets.

Failure to provide such information may result in account restriction, suspension, or termination.

11.1.7 Travel Rule Compliance BTTPL fully adheres to the Travel Rule requirement for Virtual Digital Asset (VDA) transfers. Originator and

beneficiary information must accompany all VDA transactions — both deposits and withdrawals — regardless of amount or asset type.

BTTPL reserves the right to request additional information from the User at any stage if the counterparty's originator or beneficiary information is missing, incomplete, or inconsistent with compliance standards. Transactions will not be processed unless full Travel Rule data has been reviewed and approved by the Company.

11.1.8 BTTPL may also request additional information to comply with requests or mandates issued by:

a) Statutory authorities;
b) Payment system operators or banking partners;
c) Law enforcement or supervisory agencies.

Non-compliance may lead to suspension, restriction, or account termination.

11.1.9 BTTPL reserves the right to modify, update, or revise this Policy in its sole discretion at any time, without prior written notice. Continued usage of the Platform after such modifications implies acceptance by the User.

11.2 User Obligations

11.2.1 The User agrees to submit all documents and information requested by BTTPL in a timely, accurate, and verifiable manner to enable KYC, CDD, and EDD procedures for onboarding and continued access to the Platform.

11.2.2 The User shall only use the Platform for lawful and legitimate transactions, by:

a) This KYC-AML-CFT Policy,
b) BTTPL's Terms of Use, and
c) Applicable Laws in force.

11.2.3 The User shall not use the Platform for any illegal, fraudulent, anti-national, or criminal purpose or to facilitate, finance, or support such activities.

11.2.4 The User shall not misrepresent their identity, impersonate others, or disguise beneficial ownership during onboarding or while conducting any transaction on the Platform.

11.2.5 The User shall immediately notify BTTPL of any change in their KYC-related information or identification data.

11.2.6 The User shall cooperate fully with BTTPL during any compliance review or audit and shall not obstruct or delay the provision of requested information for:

a) Risk profiling,
b) Transaction monitoring,
c) Source of funds verification,
d) Travel Rule compliance.

11.2.7 The User acknowledges that failure to comply with these obligations may result in:

- Immediate suspension or termination of their account.
- Reporting to regulatory or enforcement authorities (including FIU-IND).
- Freezing or blocking of any pending transactions or assets.

11.2.8 User Declaration: By using BTTPL's services, the User declares that:

- The information provided is true, accurate, and complete.
- They are the rightful owner or authorized operator of the funds/assets used.
- They will not conceal or misrepresent their identity, beneficial ownership, or the nature of their transactions.

12. Periodic Updation of KYC

12.1 BTTPL adopts a structured and risk-based approach for the Periodic Updation of KYC (PUKYC) to ensure all customer information, documents, and identification records are current, accurate, and in line with applicable regulatory standards.

12.2 Periodic updation is triggered:

a) Based on the risk categorization assigned to the User at onboarding or during review cycles;

b) When any KYC document expires or lapses;

c) If there is a material change in the User's profile, beneficial ownership, or contact information;

d) Upon detection of discrepancies during transaction monitoring or audit;

e) When notified by any statutory, regulatory, or enforcement authority.

12.3 The minimum frequency for periodic KYC review is as follows:

Customer Risk Category	**Review Frequency**
High-Risk Customers	Annually
Medium-Risk Customers	Annually
Low-Risk Customers	Annually

This schedule represents the minimum baseline. BTTPL reserves the right to initiate ad-hoc reviews as required by evolving risk profiles, regulatory circulars, or internal monitoring.

12.4 Users are responsible for promptly notifying BTTPL of any changes to their:

- Address;
- Identification documents;
- Beneficial ownership (for entities);
- Contact details;
- Financial or tax status.

BTTPL will require valid proof of such changes for KYC record updates.

12.5 Failure to cooperate with periodic KYC updates may result in:

- Account access restrictions;
- Transaction suspensions;
- Freezing of funds or assets;

- Reporting to FIU-IND or competent authorities.

12.6 Travel Rule Compliance Framework

BTTPL is committed to full compliance with the **Travel Rule**, as outlined under the Financial Action Task Force (FATF) Recommendations and enforced via the **AML Guidelines for Virtual Digital Asset Service Providers** issued by **FIU-IND**.

The Travel Rule ensures that accurate and verifiable information about the originator and beneficiary of a Virtual Digital Asset (VDA) transfer is exchanged between the transacting parties, and retained for regulatory reporting and anti-money laundering monitoring.

The Travel Rule applies to:

- All transfers of Virtual Digital Assets (including crypto assets) conducted via BTTPL,
- Transfers initiated from or destined to other Virtual Asset Service Providers (VASPs) or unhosted wallet addresses,
- Regardless of the transaction amount.

12.6.1 Travel Rule Data Requirements

For each VDA transfer, BTTPL shall collect, verify, and transmit (where applicable) the following minimum originator and beneficiary information:

Originator Information	**Beneficiary Information**
Name	Name
VDA Wallet Address	VDA Wallet Address
National Identifier , Tax ID (PAN)	National Identifier , Tax ID (PAN)
Originator's Address	Beneficiary Wallet Address
Customer Identification Number (CIN)	Customer Identification Number , Tax ID (PAN)
Originator's Wallet Address	

12.6.2 BTTPL's Compliance Process:

a) For outbound VDA transfers, BTTPL will ensure that the required Travel Rule information is:

- Collected at the point of transaction initiation,
- Validated against the User's KYC profile,
- Transmitted to the receiving exchange or VASP via secure channels prior to transaction execution or Destined Wallet.

b) For inbound VDA transfers, BTTPL will:

- Expect the counterparty to transmit complete Travel Rule information,
- Validate the beneficiary data against the receiving User's profile,
- Hold or reject the transaction in case of incomplete, inaccurate, or suspicious information.

12.6.3 Handling Non-Cooperative Transfers

If the required Travel Rule information is not available or cannot be verified:

- The transaction may be placed on hold, pending clarification,
- The originator or beneficiary will be contacted to provide missing information,
- BTTPL reserves the right to reject or reverse the transaction,
- Suspicious cases will be escalated internally for review and reported via an STR to FIU-IND if deemed necessary.

12.6.4 Record keeping Obligation

In accordance with PMLA, PMLR, and FATF guidelines:

- Travel Rule data must be stored securely for a minimum of **five (5) years** from the date of the transaction,

- The data must be made available for inspection by authorized regulatory bodies upon request.

12.6.4 Unhosted Wallet Risk Handling

In case the transfer involves an unhosted (non-custodial) wallet:

- The originator or beneficiary will be required to provide self-declaration, including wallet ownership confirmation,
- The transaction will be subject to Enhanced Due Diligence (EDD) before execution,
- Transfers involving high-risk jurisdictions or flagged wallets will be automatically reviewed and possibly blocked.

12.6.5 Continuous Improvement

BTTPL will periodically review its Travel Rule processes in light of:

- Regulatory updates from FIU-IND, RBI, or other competent authorities,
- Industry practices and emerging compliance tools,
- Feedback from transaction monitoring systems and post-transaction audits.

13. Internal Controls

13.1. Record Preservation and Management

13.1.1 BTTPL ensures that all customer information collected under this Policy is handled exclusively following the Terms of Use, the Privacy Policy, and Applicable Laws, including relevant data protection and security provisions.

13.1.2 The Company maintains robust technical and organizational safeguards to ensure the confidentiality, integrity, and availability of User data. These safeguards will prevent:

- Unauthorized access;
- Alteration;
- Loss or destruction;
- Disclosure or use inconsistent with lawful purposes.

13.1.3 BTTPL retains:

a) KYC documentation for all active and past Users;
b) Transaction logs, including date, amount, wallet address, transaction ID, and User account linkage;
c) Internal audit logs, suspicious transaction flags, and compliance escalation records.

13.1.4 In the event of regulatory or law enforcement requests, BTTPL shall produce:

a) Verified KYC documents;
b) Full transaction histories;
c) Audit records relating to the User's activity.

All records must be traceable, timestamped, and capable of being presented in court or regulatory proceedings.

13.1.5 BTTPL will retain all KYC, transaction, and audit-related records for a minimum period of five (5) years from:

- The date of User account closure (for identity data), or
- The date of transaction (for transaction data),

or such longer period as may be mandated by any law, regulation, or ongoing investigation.

13.1.6 In the case of legal or regulatory proceedings, all relevant records shall be retained until:

- Final resolution of the proceedings, or
- Completion of a regulatory review, even if this exceeds the 5-year standard.

13.1.7 All records must be:

- Tamper-proof.
- Securely stored, whether digital or physical.
- Readily accessible for audit or regulatory review by,

a) Internal and external auditors;
b) FIU-IND, SEBI, RBI, CERT-In, or other supervisory bodies and

advisory bodies;
c) Law enforcement agencies upon lawful request.

14. Audit and Compliance

14.1 BTTPL is committed to maintaining a robust and compliance framework to ensure complete adherence to its obligations under the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PMLR), the AML Guidelines for Virtual Digital Asset Service Providers (FIU-IND), and globally accepted standards including those recommended by the Financial Action Task Force (FATF).

14.2 BTTPL shall conduct periodic internal audits and compliance reviews to evaluate the effectiveness of its KYC-AML-CFT framework. These reviews will focus on:

- The adequacy and enforcement of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) measures;
- Completeness and ongoing accuracy of customer identification and verification records;
- Operational performance of transaction monitoring systems, including alert generation, review, and closure;
- Timely and accurate filing of Suspicious Transaction Reports (STRs) and other required reports;
- Adherence to sanctions screening and blacklisting policies;
- Compliance with the Travel Rule for Virtual Digital Asset transfers.

14.3 Internal audits will be conducted by competent, independent teams or outsourced third-party specialists with relevant expertise. Audit results will be submitted to the Company's Designated Director and senior management for assessment and decision-making.

14.4 The Company's senior management, including the Designated Director and Principal Officer, will evaluate all audit findings and initiate corrective actions such as:

- Policy or process improvements;
- Implementation of new risk controls;
- Employee training or retraining;

- System upgrades or modifications to ensure AML/CFT compliance.

14.5 The Designated Director will ensure that significant audit observations and their corresponding remediation plans are reported to the Board of Directors to promote top-level oversight of the Company's AML-CFT compliance posture.

14.6 The audit cycle will follow a risk-based frequency, but will occur at a minimum:

- Annually for the end-to-end AML-CFT compliance framework;
- Semi-annually for transaction monitoring system efficiency;
- On-demand if significant operational changes, product updates, or financial crime typologies emerge.

14.7 All audit reports, supporting logs, remediation plans, and closure notes shall be securely retained for a minimum period of five (5) years, or as extended by Applicable Law or regulatory instruction.

15. Regulatory Reporting to FIU-IND

15.1 BTTPL is fully committed to meeting its reporting obligations under the PMLA, PMLR, and relevant regulatory circulars issued by the Financial Intelligence Unit – India (FIU-IND).

15.2 The following reporting obligations apply under this Policy:

a) Suspicious Transaction Report (STR): All transactions, whether completed or merely attempted, that raise suspicion of criminal activity, money laundering, terrorist financing, fraud, or other illegal purposes shall be investigated. If deemed suspicious, an STR shall be submitted to the FIU-IND.

- **Submission Timeline:**
  Within **seven (7) working days** from the date of concluding that a transaction is suspicious.

b) Non-Profit Organisation Transaction Reports (NTR): Where applicable, transactions involving Non-Profit Organisations above prescribed thresholds will be disclosed, following regulatory formats and timelines.

15.3 BTTPL will fully cooperate with regulatory, supervisory, and law enforcement authorities during inspections, audits, and formal requests for information. The Company will provide additional clarifications or documentary support upon request by FIU-IND.

15.4 All submitted STRs, along with their supporting investigation records, will be retained for five (5) years from the date of submission or transaction completion, whichever is later.

15.5 The obligation to report also applies to attempted transactions or any pattern of behavior fitting a recognized suspicious typology — even if the transaction is not completed.

15.6 All employees are obligated to escalate any suspicion of illegal, fraudulent, or suspicious transactions to the Principal Officer or the Compliance Team, who will assess the matter and, if necessary, prepare the required regulatory filings.

16. Employee Training & Awareness Policy Statement

At Beamer Trades and Technologies (OPC) Pvt. Ltd. (BTTPL), we recognize that an effective Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) program is driven not only by strong systems and procedures, but by well-informed and vigilant employees who understand the significance of their role in protecting the Company and its stakeholders from financial crime risks.

BTTPL is committed to developing and sustaining a workplace culture where compliance, ethical behavior, and regulatory awareness are an integral part of daily decision-making. To uphold this standard, the Company has implemented a comprehensive, structured, and dynamic Employee Training & Awareness Framework.

The objectives of this Training Program are to:

- Ensure all employees understand the nature and scope of money laundering, terrorist financing, and fraud risks, including the potential legal and reputational consequences of non-compliance.
- Equip staff with the knowledge of applicable laws, rules, guidelines, and internal procedures, particularly the Prevention of Money

Laundering Act, 2002 (PMLA), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PMLR), and the AML Guidelines for Virtual Digital Asset Service Providers issued by FIU-IND.

- Strengthen employees' ability to recognize red flag indicators, unusual patterns of customer behavior, and emerging typologies of financial crime.
- Promote the accurate and timely escalation of suspicious transactions to the designated Compliance Officers.
- Ensure the Company's compliance obligations are consistently met through the knowledge, competency, and ethical conduct of its personnel.

BTTPL's commitment to ongoing training extends beyond initial onboarding and ensures that all relevant employees are regularly updated on regulatory changes, risk trends, and emerging global compliance standards through structured annual programs, specialized workshops, and targeted refresher sessions.

All employees must treat participation in this training as a professional responsibility and are expected to apply the knowledge in their daily activities, thereby reinforcing the integrity and regulatory compliance of the Company at all times.

17. Employee Training & Awareness Framework

17.1 Purpose & Commitment BTTPL acknowledges that an informed, vigilant, and compliant workforce is fundamental to safeguarding against money laundering, terrorist financing, and other forms of financial crime. The Company is committed to maintaining a structured and auditable training framework designed to ensure all employees are fully aware of their responsibilities under applicable legal and regulatory frameworks including:

- The Prevention of Money Laundering Act, 2002 (PMLA)
- The Prevention of Money Laundering Rules (PMLR)
- Financial Intelligence Unit – India (FIU-IND) Guidelines

- FATF Recommendations and Industry Best Practices

17.2 Objectives The primary objectives of this framework are to:

- Foster a culture of risk-awareness, accountability, and compliance at all levels.
- Ensure employees understand their role in identifying, preventing, and reporting suspicious activity.
- Provide continuous learning to adapt to emerging risks, regulatory changes, and enforcement trends.

17.3 Scope: Who Must Undergo Training The training framework applies to all employees based on the nature of their roles:

Category	**Training Frequency**	**Examples of Roles**
Customer-facing Staff	Induction + Annual + Event-based	Sales, Relationship Managers, Onboarding Teams
Operations & Transaction Teams	Induction + Annual + Event-based	Payment Processing, Settlements, Risk Ops
Compliance & Audit Personnel	Induction + Annual + Event-based	Compliance Officers, Risk Analysts, Auditors
Senior Management & Board	Annual + Event-based	Directors, Executive Officers
Support Functions (IT, HR, Admin)	Induction + Biennial + Event-based	Software Devs, HR, Admin

17.4 Delivery Methodology Training will be imparted through a combination of:

1. **E-Learning Modules:** Interactive courses with embedded quizzes and practical scenarios.
2. **In-Person Workshops / Seminars:** Led by compliance experts, especially for new hires and regulatory updates.
3. **Webinars and Video Tutorials:** For specialized topics or emerging financial crime typologies.
4. **On-the-Job Coaching:** For high-risk or specialized roles, delivered by team leads or compliance personnel.

17.5 Assessment and Certification

- Upon completion of each training module, employees will undergo an online or written assessment to verify knowledge retention.
- The **minimum passing score is set at 80%** for all compliance-critical roles.
- Employees failing to meet the passing criteria will be required to retake the module until they pass.
- All assessments will be logged and stored in employee records for at least **5 years**, as part of compliance documentation.

17.6 Retraining and Refresher Programs

Trigger for Retraining	**Timeframe for Completion**
Annual Recertification (all roles)	Within calendar year
Regulatory Change (e.g., PMLA amendment, FIU circular)	Within 30 days of notification
Internal Policy Update or System Change	Prior to rollout or go-live
Audit or Compliance Breach Identified	As directed by Compliance Head (usually within 15 days)
Employee Reassignment to New Risk-Exposure Role	Before assuming new responsibilities

17.7 Documentation and Records Management

The following records will be maintained by the Compliance Department:

- Training Attendance Logs
- Assessment Results
- Employee Certification Status
- Updated Training Content (version-controlled)
- Record of Non-Compliance and Corrective Actions

All records shall be retained for **at least 5 years** or as specified by applicable laws.

17.8 Enforcement & Corrective Measures

- Failure to complete mandatory training within the prescribed timeline will trigger automatic suspension of access to systems

related to customer data or transaction processing until compliance is achieved.

- Repeated non-compliance or failure to pass assessments may result in disciplinary action up to and including termination, in line with the Company's HR and disciplinary policies.

17.9 Continuous Learning Culture

BTTPL fosters ongoing compliance awareness via:

- Monthly newsletters summarizing relevant regulatory updates and financial crime news.
- Periodic policy update notifications.
- Encouragement to attend external seminars, webinars, and industry networking events related to AML-CFT and risk management.

18. Tipping Off

18.1 Legal Framework

BTTPL (the "Company") and its employees are bound by:

- Prevention of Money-Laundering Act (2002) – s.12 & s.13
- Financial Intelligence Unit–India (FIU-IND) Guidelines – Ch. 4, para 3
- FATF Recommendation 21 – "Tipping-off and confidentiality"

These provisions *expressly prohibit* disclosing to a customer, or any unauthorised party, that:

1. A Suspicious Transaction Report (STR) is being considered, prepared, or has been filed; or
2. An investigation, inquiry, or other enforcement action is under way.

18.2 Definition

"Tipping-off" means any act, intentional or inadvertent, that could make a customer (or related third party) aware that they are the subject of:

- An STR,

- Ongoing internal or regulatory investigation, or
- Enhanced monitoring triggered by the Company's AML/CFT controls.

18.3 Confidentiality Obligations

1. **Need-to-Know Principle STR preparation, filing, and follow-up may only be discussed with:**
    - the Principal Officer (PO) and designated AML team members;
    - senior management on a need-to-know basis;
    - legal counsel (internal or external) under privilege;
    - FIU-IND or other competent authorities.

2. **Record Handling** All STR-related files are stored in the restricted "AML-STR" vault with role-based access controls (RBAC).
3. **System Flags** Case identifiers in transaction-monitoring tools must not be visible to front-line staff who interact with the customer.

18.4 Customer & Third-Party Communication Protocol

Scenario	Permitted Response
Customer asks why an outgoing withdrawal is delayed / on hold	"Your transaction is undergoing routine compliance review. We'll update you once processing is complete." *(No mention of STR or suspicion.)*
Law-enforcement or regulator requests information	Refer immediately to the PO. Respond only through approved channels and within statutory time-frames.
Media or social-media inquiry	"No comment." Forward to Compliance & Communications team.

18.5 Exceptions

Disclosure is allowed *only* when:

- Required by a court order or other binding legal process and cleared by Company counsel, or
- Directed in writing by FIU-IND or another competent authority.

18.6 Employee Responsibilities

1. Immediate Escalation Any suspected or attempted tipping-off must be reported to the PO within 24 hours.
2. Secure Conversations Discuss STR matters only in approved secure channels (designated email group, encrypted messenger, or in-person in compliance office).
3. Documentation Maintain an audit trail of all communications related to STR processing.

18.7 Monitoring & Assurance

- Quarterly sample testing of STR workflows by Internal Audit
- Key Risk Indicator (KRI): "Number of confirmed tipping-off incidents" – tolerance = 0.

18.8 Disciplinary & Legal Consequences

- Internal Breaches constitute gross misconduct and may lead to dismissal.
- Regulatory Section 13, PMLA: imprisonment up to 3 years and/or monetary penalty.
- Civil/Criminal Company reserves the right to pursue damages for losses arising from unauthorised disclosure.