Anti-Money Laundering (AML) Policy

1. Introduction

Bright Carrier Technology Pvt. Ltd. (“BriteX,” “we,” “us,” or “our”) is committed to maintaining strong Anti-Money Laundering (AML) controls and preventing the use of its cryptocurrency exchange platform for money laundering, terrorist financing, fraud, sanctions evasion, or other illicit activities.

2. Regulatory Compliance

BriteX complies with applicable AML, counter-terrorist financing, and reporting obligations, including:

- The Prevention of Money Laundering Act, 2002 (PMLA), India
- Financial Action Task Force (FATF) recommendations
- Applicable Reserve Bank of India (RBI) guidance, where relevant
- Other applicable domestic and international AML, sanctions, and financial crime regulations

3. Customer Due Diligence

3.1 Know Your Customer Requirements

All users must complete KYC verification before they are permitted to:

- Make deposits or withdrawals
- Trade cryptocurrencies
- Access advanced platform features such as futures, staking, or other restricted services

Required KYC documents may include:

- Government-issued photo identification, such as Aadhaar, PAN, passport, or driving license
- Proof of address issued within the previous three months
- Selfie or live-liveness verification
- Additional documents requested by BriteX or required by regulatory authorities

3.2 Enhanced Due Diligence

Enhanced due diligence may be required for customers, accounts, or transactions involving:

- High-value transactions above ₹10,00,000 or equivalent

- Politically Exposed Persons (PEPs) and related parties
- Customers or counterparties from high-risk jurisdictions
- Unusual, complex, or suspicious transaction patterns

4. Transaction Monitoring

BriteX uses risk-based transaction monitoring controls, including:

  - Real-time transaction monitoring systems
  - Automated suspicious activity detection tools
  - Daily and risk-based transaction limits based on verification level
  - Manual compliance review of alerts and escalations where required

5. Suspicious Transaction Reporting

BriteX reviews and reports suspicious activity in accordance with applicable laws and regulatory timelines. Reports may be submitted to:

  - Financial Intelligence Unit - India (FIU-IND)
  - Other competent regulatory or law enforcement authorities, where required
  - Relevant authorities within prescribed regulatory timelines

6. Recordkeeping

BriteX maintains AML and customer records securely for the minimum period required by law, including:

  - Customer identification and verification records for at least five years after account closure
  - Transaction records for at least five years from the transaction date
  - Suspicious Transaction Reports and supporting documentation for at least five years

7. Risk Assessment

BriteX applies a risk-based approach to customer and transaction review. Customer risk categories include:

  - **Low Risk:** Regular retail users with completed and verified KYC
  - **Medium Risk:** High-volume traders, business accounts, or users requiring additional monitoring
  - **High Risk:** PEPs, customers connected to high-risk jurisdictions, or users displaying unusual activity patterns

8. Training and Awareness

BriteX provides AML and compliance training to relevant employees, including:

- Initial AML training upon joining
- Annual refresher training
- Updates on regulatory and policy changes
- Role-specific compliance training for employees handling customers, transactions, investigations, or reporting

9. Prohibited Activities

Users are prohibited from using BriteX to:

- Provide false, forged, misleading, or incomplete identification information
- Conduct transactions on behalf of another person without proper authorization
- Structure, split, or manipulate transactions to avoid monitoring or reporting requirements
- Use the platform for illegal, fraudulent, sanctioned, or prohibited activities

10. AML Compliance Officer

AML Compliance Officer Contact

Email: bctechpvtltd0120@gmail.com

Phone: 03474 353034

This policy may be reviewed and updated periodically to reflect changes in applicable laws, regulatory guidance, business operations, or internal risk controls.