docree.

AML / KYC Policy

COMPANY	Docree Demo Exchange Ltd
REGISTRATION	HE 000000
EFFECTIVE DATE	November 28, 2026
VERSION	v1.0

Table of Contents

01 Introduction & Scope
02 Customer Due Diligence
03 Enhanced Due Diligence
04 Transaction Monitoring
05 Travel Rule Compliance
06 Sanctions & PEP Screening
07 Suspicious Activity Reporting
08 Record Keeping & Staff Training

SECTION 01

Introduction & Scope

1.1 Docree Demo Exchange (the "Company") maintains this Anti-Money Laundering and Know Your Customer Policy (the "Policy") to prevent the use of its platform for money laundering, terrorist financing, sanctions evasion, and other financial crimes.

1.2 This Policy applies to all employees, contractors, and agents of the Company, and to all customers, transactions, and services offered through the platform.

SECTION 02

Customer Due Diligence

2.1 Before a customer may trade or withdraw funds, the Company performs Customer Due Diligence ("CDD") to verify their identity. Required information includes:

- Full legal name, date of birth, nationality, and residential address.
- Government-issued photo identification (passport, national ID, driver's license).
- Proof of address (utility bill or bank statement less than 90 days old).
- Selfie with liveness check to confirm the ID belongs to the customer.
- For corporate customers: certificate of incorporation, ownership structure, UBOs.

2.2 The Company uses automated identity verification services and manual review to validate the authenticity of documents and the identity of the customer.

SECTION 03

Enhanced Due Diligence

3.1 Enhanced Due Diligence ("EDD") is applied to customers who present higher risk, including:

- Politically Exposed Persons (PEPs) and their associates.
- Customers from high-risk jurisdictions (FATF grey/black list countries).
- High-net-worth customers with trading volumes exceeding $100,000/month.
- Customers whose source of funds is unclear or appears inconsistent with activity.
- Corporate customers with complex or opaque ownership structures.

3.2 EDD measures include: source of funds and wealth declarations, additional ID verification, senior management approval for account opening, and enhanced ongoing monitoring.

SECTION 04

Transaction Monitoring

4.1 The Company continuously monitors customer transactions to detect unusual or suspicious patterns. Red flags include:

- Rapid deposit followed immediately by withdrawal (layering).
- Structuring transactions just below reporting thresholds.
- Transactions inconsistent with the customer's stated profile.
- Deposits from mixers, tumblers, or blockchain privacy tools.
- Wallet addresses associated with darknet markets, scams, ransomware, or hacks.

SECTION 05

Travel Rule Compliance

5.1 In accordance with FATF Recommendation 16 (the "Travel Rule"), the Company collects and transmits originator and beneficiary information for cryptocurrency transfers exceeding the applicable threshold (typically $1,000 USD equivalent).

5.2 Travel Rule information shared between Virtual Asset Service Providers (VASPs) includes: originator name, account number/wallet address, physical address, and beneficiary name. Transfers to non-compliant counterparty VASPs may be restricted or blocked.

SECTION 06

Sanctions & PEP Screening

6.1 All customers are screened at onboarding and on an ongoing basis against international sanctions lists (OFAC, UN, EU, UK) and PEP databases. Matches trigger immediate account freezing pending investigation.

6.2 Wallet addresses are screened through blockchain analytics providers before each deposit or withdrawal. Addresses associated with sanctioned entities or illicit activity are blocked.

SECTION 07

Suspicious Activity Reporting

7.1 The Company's Money Laundering Reporting Officer (MLRO) is responsible for filing Suspicious Activity Reports (SARs) with the relevant Financial Intelligence Unit when there is reasonable grounds to suspect money laundering or terrorist financing.

7.2 The Company is legally prohibited from notifying the customer that a SAR has been filed ("tipping off"). Accounts subject to a SAR may be frozen pending law enforcement investigation.

SECTION 08

Record Keeping & Staff Training

8.1 The Company retains all CDD records, transaction logs, SARs, and correspondence for a minimum of seven (7) years from the date of the transaction or account closure.

8.2 All employees undergo AML training at onboarding and annually thereafter. Training covers regulatory requirements, red-flag identification, escalation procedures, and recent enforcement actions.

Document	AML / KYC Policy
Company	Docree Demo Exchange Ltd
Effective Date	November 28, 2026
MLRO Contact	compliance@docree.com

© 2026 Docree Demo Exchange. All rights reserved.

docree.

Generated at docree.com — Powered by Brokeret Solutions