docree.

AML/KYC Policy

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

Table of Contents

01 Introduction

02 Definitions

03 Customer Verification

04 Enhanced Verification

05 Ongoing Monitoring

06 Record Keeping

07 Sanctions Screening

08 Client Non-Compliance

SECTION 01

Introduction

1.1 Docree Demo Funding Ltd, trading as Docree Demo Funding (hereinafter referred to as "the Company"), is committed to the highest standards of Anti-Money Laundering ("AML") and Counter-Terrorist Financing ("CTF") compliance. This policy sets out the Company's procedures for preventing the use of its services for money laundering, terrorist financing, or other financial crimes.

1.2 Although the Company operates a proprietary trading evaluation program rather than a traditional brokerage, the Company recognizes the importance of robust identity verification and anti-money laundering controls. Evaluation fees, profit payouts, and refunds represent financial flows that must be monitored and controlled in accordance with applicable laws.

1.3 This policy applies to all officers, employees, contractors, and agents of the Company. All personnel are required to familiarize themselves with this policy and to comply with its provisions in the performance of their duties.

1.4 The Company has appointed a designated compliance officer who is responsible for overseeing the implementation of this policy, receiving internal reports of suspicious activity, and filing external reports with the relevant authorities as required by law.

1.5 The Company's compliance department can be contacted at compliance@docree.com for any questions or concerns relating to this policy.

SECTION 02

Definitions

Money Laundering

The process by which criminals attempt to conceal the true origin, ownership, or destination of illegally obtained funds by channelling them through legitimate financial systems or commercial activities.

Terrorist Financing

The provision, collection, or management of funds with the intention or knowledge that such funds will be used to carry out terrorist acts or to support terrorist organizations.

Customer Due Diligence (CDD)

The process of identifying and verifying the identity of a Participant, understanding the nature and purpose of the business relationship, and assessing the money laundering and terrorist financing risk associated with the Participant.

Enhanced Due Diligence (EDD)

Additional verification measures applied to Participants or transactions that present a higher risk of money laundering or terrorist financing.

Politically Exposed Person (PEP)

An individual who is or has been entrusted with a prominent public function, including heads of state, senior government officials, senior judicial or military officials, senior executives of state-owned corporations, and important political party officials, as well as their immediate family members and close associates.

Beneficial Owner

The natural person(s) who ultimately own or control a Participant entity and/or the natural person on whose behalf a transaction or activity is being conducted, including any person exercising ultimate effective control over a legal entity or arrangement.

Suspicious Activity Report (SAR)

A report filed internally with the compliance officer or externally with the relevant authority when there are reasonable grounds to suspect that a transaction or activity may be related to money laundering or terrorist financing.

Participant

Any individual or entity that registers for an account with the Company for the purpose of purchasing an evaluation, participating in the evaluation program, or operating a funded trading account.

2.1 The definitions set out above shall apply throughout this policy unless the context otherwise requires. Terms defined in applicable legislation shall have the meanings ascribed to them in such legislation.

SECTION 03

Customer Verification

3.1 The Company shall conduct identity verification on all prospective Participants before activating their account or processing any evaluation purchase. No evaluation account shall be provided until the verification process has been satisfactorily completed, unless the Company permits limited access pending verification at its sole discretion.

3.2 Identity Verification

3.2.1 The identity verification process requires the collection and verification of the following information for individual Participants:

- Full legal name as it appears on an official government-issued identification document;
- Date of birth;
- Nationality and country of residence;

- Residential address (not a P.O. Box);
- Valid government-issued photo identification — at least one of the following: passport, national identity card, or driving licence. The document must be current, unaltered, and clearly legible;
- A selfie or live photograph for biometric comparison with the identification document, where required by the Company's verification process.

3.3 Proof of Address

3.3.1 The Company requires proof of the Participant's residential address. Acceptable documents include:

- Utility bill (electricity, gas, water, telephone, or internet) issued within the last three (3) months;
- Bank account statement or credit card statement issued within the last three (3) months;
- Government-issued correspondence (tax notice, electoral registration, or similar) issued within the last twelve (12) months;
- Official residence certificate or proof of address letter issued by a government authority.

3.3.2 The proof of address document must display the Participant's full name and residential address, and must match the information provided during registration. Documents must be clearly legible and unaltered.

3.4 Payment Method Verification

3.4.1 The Company may require verification of the payment method used to purchase an evaluation to ensure that the payment instrument belongs to the registered Participant. This may include:

- A photograph or screenshot of the front of the payment card showing the last four digits, cardholder name, and expiry date (with the full card number obscured);
- A screenshot or confirmation of the electronic wallet account showing the Participant's name and account identifier;
- A bank transfer confirmation showing the sender's name and account details.

3.4.2 The Company does not accept payments from third parties. All evaluation fee payments must originate from a payment instrument registered in the name of the Participant. Similarly, all profit payouts on funded accounts will be made only to payment instruments in the Participant's name.

3.5 The Company reserves the right to request additional documentation or information at any time during the business relationship if it considers such information necessary to fulfil its verification obligations.

3.6 Where the Company is unable to complete the verification process to its satisfaction, it shall not activate the account, shall not process any evaluation purchases, and may consider filing a Suspicious Activity Report with the relevant authority.

SECTION 04

Enhanced Verification

4.1 The Company shall apply Enhanced Due Diligence measures in circumstances where the risk of money laundering or terrorist financing is assessed as higher than normal. EDD shall be applied, at a minimum, in the following situations:

- The Participant is a Politically Exposed Person (PEP), a family member of a PEP, or a known close associate of a PEP;
- The Participant is resident in, or the payment originates from, a country or jurisdiction identified as high-risk by the FATF or by the Company's own risk assessment;
- The Participant's transaction patterns are inconsistent with their stated profile (for example, purchasing multiple high-value evaluations in rapid succession);
- There are grounds for suspicion that the Participant's funds are derived from criminal activity;
- The Participant requests unusually large or frequent profit payouts that are inconsistent with their funded account activity.

4.2 Enhanced Due Diligence measures may include, but are not limited to:

- Obtaining additional identification documents or information from independent and reliable sources;
- Conducting enhanced background checks using reputable third-party databases and screening services;
- Requiring a detailed explanation of the source of funds used to purchase evaluations, supported by documentary evidence;
- Obtaining senior management approval before activating the account or processing payouts;
- Increasing the frequency and intensity of ongoing monitoring of the Participant's activity.

4.3 The Company shall document the rationale for applying EDD, the additional measures taken, and the outcome of those measures. All EDD records shall be retained in accordance with the Company's record-keeping obligations.

4.4 Where the EDD process reveals information that gives rise to suspicion of money laundering or terrorist financing, the matter shall be escalated immediately to the compliance officer for assessment and, if appropriate, the filing of a Suspicious Activity Report.

SECTION 05

Ongoing Monitoring

5.1 The Company shall conduct ongoing monitoring of all Participant accounts and transactions to ensure that they are consistent with the Company's knowledge of the Participant, their stated profile, and the expected use of the services.

5.2 Ongoing monitoring includes, but is not limited to:

- Monitoring evaluation purchases, payment patterns, and payout requests for anomalies or inconsistencies with the Participant's profile;
- Monitoring for patterns that may indicate abuse of the evaluation program, including rapid cycling of purchases and refund requests, or use of multiple identities or accounts;
- Periodic review and updating of Participant identification documents and verification information, particularly for funded traders receiving regular profit payouts;
- Regular screening of Participants against updated sanctions lists, PEP databases, and adverse media sources;
- Monitoring funded account activity for unusual trading patterns that may indicate the account is being used for purposes other than legitimate trading.

5.3 The frequency and depth of ongoing monitoring shall be commensurate with the risk level assigned to the Participant. Higher-risk Participants shall be subject to more frequent and intensive monitoring.

5.4 Any unusual or suspicious activity identified through ongoing monitoring shall be reported promptly to the compliance officer for further investigation and determination of whether a Suspicious Activity Report should be filed with the relevant authority.

5.5 The Company may suspend, restrict, or close a Participant's account pending the outcome of an investigation, where it considers such action necessary to comply with its legal obligations or to protect the integrity of its operations.

SECTION 06

Record Keeping

6.1 The Company shall maintain comprehensive records of all verification information, transaction data, internal and external suspicious activity reports, and any other documentation obtained in the course of fulfilling its AML/KYC obligations.

6.2 All records shall be retained for a minimum period of five (5) years from the date the business relationship ends, or from the date the transaction is completed, whichever is later, unless a longer retention period is required by applicable law or regulation.

6.3 Records shall be stored securely and shall be readily accessible to the compliance officer and any competent regulatory or law enforcement authority upon lawful request.

6.4 The Company shall ensure that its record-keeping systems are adequate to reconstruct individual transactions, including evaluation purchases, refunds, and profit payouts — recording amounts, currencies, dates, payment methods, and parties involved — so as to provide an audit trail for any investigation or regulatory inquiry.

6.5 Records of Suspicious Activity Reports, whether filed internally or externally, shall be retained securely and separately from general Participant records. Access to SAR records shall be restricted to the compliance officer and authorised personnel only.

SECTION 07

Sanctions Screening

7.1 The Company shall screen all prospective and existing Participants against applicable sanctions lists, including but not limited to lists maintained by the United Nations Security Council, the European Union, the United States Office of Foreign Assets Control (OFAC), His Majesty's Treasury (HMT), and any other relevant national or supranational authority.

7.2 Sanctions screening shall be performed at the point of account registration, upon any change to Participant information, and on a periodic basis as determined by the Company's risk assessment.

7.3 Where a potential match is identified against a sanctions list, the Company shall immediately escalate the matter to the compliance officer for further investigation. No evaluation purchases shall be processed and no payouts shall be made for the Participant until the matter has been resolved.

7.4 If a confirmed match is established, the Company shall take all necessary steps to comply with the applicable sanctions regime, which may include freezing the Participant's account and any pending payouts, declining to process transactions, terminating the business relationship, and reporting the matter to the relevant authority.

7.5 The Company shall maintain up-to-date sanctions screening tools and databases and shall ensure that its screening processes are commensurate with its risk profile and the jurisdictions in which it operates.

SECTION 08

Client Non-Compliance

WARNING

Providing false, misleading, or incomplete information during the verification process, or using the Company's services for money laundering, terrorist financing, or any other financial crime, is a serious offence that may result in account termination, withholding of payouts, and referral to law enforcement authorities.

8.1 Participants are required to provide accurate, complete, and up-to-date information during the account registration process and at any time the Company requests updated documentation. Failure to do so may result in the restriction or suspension of the Participant's account until the required information is provided.

8.2 The Company shall take appropriate action against any Participant who is found to have provided false, misleading, or incomplete information during the verification process, or who is found to be

using the Company's services for the purpose of money laundering, terrorist financing, or any other financial crime. Such action may include:

- Immediate suspension or termination of the Participant's account;
- Withholding of any pending evaluation fee refunds or profit payouts pending investigation;
- Voiding any evaluation progress or funded account allocation obtained through fraudulent means;
- Reporting the matter to the relevant regulatory and law enforcement authorities;
- Pursuing civil remedies to recover any losses suffered by the Company.

8.3 Participants who refuse to provide requested identification documents, proof of address, payment method verification, or other information required for the verification process shall have their account functionality restricted. Profit payouts may be withheld until the Company is satisfied that all verification requirements have been met.

8.4 This policy is subject to periodic review and may be updated to reflect changes in applicable laws, regulations, or the Company's risk assessment. Participants will be notified of any material changes via the Company's website or by email.

Document	AML/KYC Policy
Company	Docree Demo Funding Ltd
Effective Date	November 28, 2026
Website	https://docree.com
Compliance Contact	compliance@docree.com

© 2026 Docree Demo Funding. All rights reserved.

docree.
Generated at docree.com — Powered by Brokeret Solutions