docree.

AML Program

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

Table of Contents

01 Program Overview
02 Governance & MLRO
03 Customer Onboarding (KYB/KYC)
04 Risk-Based Classification
05 Transaction Monitoring
06 Sanctions Screening
07 Suspicious Activity Reporting
08 Training & Record Keeping

SECTION 01

Program Overview

1.1 Docree Demo Payments (the "Company") maintains a comprehensive Anti-Money Laundering Program (the "Program") to prevent, detect, and report money laundering, terrorist financing, and sanctions evasion through its payment-processing services.

1.2 The Program is designed to comply with applicable AML laws including the Bank Secrecy Act, the USA PATRIOT Act, FATF Recommendations, EU AML Directives, and local regulations in the jurisdictions where the Company operates.

SECTION 02

Governance & MLRO

2.1 The Company has designated a Money Laundering Reporting Officer ("MLRO") with overall responsibility for the Program. The MLRO reports directly to the board or executive management on AML matters and has independent authority to escalate concerns.

2.2 The MLRO's responsibilities include:

- Maintaining the AML Program and ensuring it is fit for purpose.
- Reviewing internal SARs and filing them with the relevant Financial Intelligence Unit.
- Overseeing sanctions, PEP, and adverse-media screening.
- Coordinating independent AML audits and regulatory examinations.
- Delivering AML training to staff.

SECTION 03

Customer Onboarding (KYB/KYC)

3.1 All merchants and users must complete identity verification before receiving services. For business (KYB) onboarding, the Company collects:

- Certificate of incorporation and good standing.
- Memorandum and articles of association.
- Register of directors and shareholders.

- Identification of Ultimate Beneficial Owners (UBOs) holding 25% or more.
- Proof of registered and operating addresses.
- Business model, expected transaction volume, and target markets.

3.2 For individual (KYC) onboarding, the Company collects government-issued photo ID, proof of address, and a selfie with liveness check.

SECTION 04

Risk-Based Classification

4.1 Each customer is assigned a risk rating at onboarding (Low / Medium / High) based on:

- Geographic risk (country of registration, operations, and target markets).
- Industry risk (business type, regulated status, historical fraud rates).
- Customer risk (PEP status, adverse media, prior compliance issues).
- Product/channel risk (payment methods, currencies, settlement destinations).

4.2 Enhanced Due Diligence (EDD) is mandatory for all high-risk customers and includes source of funds documentation, senior-management approval, and enhanced ongoing monitoring.

SECTION 05

Transaction Monitoring

5.1 The Company monitors all transactions through automated rule-based and behavioral analytics systems. Monitoring rules include:

- Velocity thresholds (transaction count, value, and frequency).
- Structuring patterns (transactions just below reporting thresholds).
- High-risk geography corridors.
- Mismatches between declared business activity and actual transaction patterns.
- Rapid in-and-out (pass-through) flows.
- Chargeback and refund spikes indicating fraud.

SECTION 06

Sanctions Screening

6.1 All customers, beneficial owners, and counterparties are screened at onboarding and continuously thereafter against:

- OFAC Specially Designated Nationals (SDN) list.
- UN Security Council Consolidated List.
- EU Consolidated List of Sanctions.
- UK HM Treasury Consolidated List.
- PEP databases and adverse media.

6.2 Positive matches trigger immediate account freezing pending investigation. Confirmed matches result in termination and reporting as required by law.

SECTION 07

Suspicious Activity Reporting

7.1 Employees must escalate suspicious activity to the MLRO through the internal SAR process. The MLRO reviews internal SARs and files external SARs with the relevant Financial Intelligence Unit where thresholds are met.

7.2 The Company prohibits “tipping off”: no employee may disclose to a customer that they are the subject of a SAR or investigation. Violators face disciplinary action and potential criminal liability.

SECTION 08

Training & Record Keeping

8.1 All employees complete mandatory AML training at onboarding and annually thereafter. High-risk roles (underwriting, compliance, customer support) receive enhanced training.

8.2 The Company retains all AML records — including CDD files, transaction data, SARs, and internal investigations — for a minimum of five (5) to seven (7) years from the date of the transaction or account closure, per local regulatory requirements.

Document	AML Program
Company	Docree Demo Payments Ltd
Effective Date	November 28, 2026
MLRO Contact	compliance@docree.com

© 2026 Docree Demo Payments. All rights reserved.

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