AML/KYC Policy

1. Introduction

This Anti-Money Laundering and Know Your Customer (AML/KYC) Policy is established by Vault Fintech Solutions s.r.o. ("Vault", "the Company", "we", or "us") to prevent the Company's involvement in illicit financial activities and to ensure compliance with applicable laws and regulations. This policy may be amended from time to time to reflect legislative developments and best global practices in AML and KYC compliance.

Vault complies with laws and standards aimed at combatting money laundering and the financing of terrorism.

2. Definitions

Beneficial Owner: Any natural person who ultimately owns or controls a User or on whose behalf a transaction is conducted. This includes, but is not limited to, those owning more than 25% of a company's shares or voting rights, or who otherwise exercise control through other means. Where no beneficial owner is identified, the senior managing official may be considered as the beneficial owner.

Politically Exposed Person (PEP): A person who holds or has held a prominent public function, as well as their immediate family members and close associates. This includes heads of state, senior politicians, judges, military officers, and executives of state-owned enterprises.

Sanctioned Jurisdiction: Any country or territory subject to international sanctions issued by the UN, US, EU, or equivalent.

Prohibited Jurisdiction: Any jurisdiction deemed by Vault as restricted for offering or receiving services due to high risk.

High-Risk Jurisdiction: Countries identified by Vault, FATF, or other regulatory bodies as posing significant AML/CFT risk.

3. Initial and Ongoing Screening

Vault performs thorough due diligence on all users during onboarding and continuously throughout the business relationship. This includes screening against global sanctions lists and monitoring transactional behavior to identify irregularities. Suspicious or high-risk activity may result in service denial, delayed transactions, or reporting to regulators.

4. KYC/AML Identification Procedures

Vault applies a risk-based approach in line with legal obligations. We identify and verify users' identities using reliable independent documentation. This includes gathering information about the nature of the relationship, source of funds, and beneficial ownership where applicable.

For individuals: Identification is verified using official documents such as a passport, ID card, or driver's license.
For legal entities: Documentation includes incorporation certificates, organizational structure, and director and shareholder information.

If identification is performed remotely, enhanced verification measures are applied, including video calls and notarized translations where necessary.

5. Ongoing Monitoring of Users

Vault regularly reviews and updates user information and monitors transactions to ensure consistency with users' risk profiles. We perform enhanced scrutiny for high-value or unusual activity, and reassess user risk based on updated data and transaction behavior.

Transactions equal to or exceeding €500 will undergo Enhanced Due Diligence (EDD), including checks on the source of funds and wealth. Real-time monitoring tools and compliance oversight by the Money Laundering Reporting Officer (MLRO) support effective risk management.

6. Sanctioned, Prohibited, and High-Risk Jurisdictions

Vault maintains lists of sanctioned, prohibited, and high-risk jurisdictions. These lists are based on assessments by FATF and other regulatory bodies. Users associated with sanctioned or prohibited jurisdictions are not permitted to use Vault's services. Users from high-risk jurisdictions are subject to enhanced due diligence.

7. High-Risk Situations

For users deemed high-risk—such as those from high-risk jurisdictions or who are politically exposed—Vault will apply enhanced due diligence. This includes senior management approval, verification of the source of funds and wealth, and ongoing scrutiny of the business relationship.

8. Record-Keeping

Vault retains transaction and user identification records for a minimum of ten (10) years, in compliance with MiCA and AML regulatory obligations. This ensures adequate evidence for any future investigations or regulatory audits.

9. Money Laundering Reporting Officer (MLRO)

The MLRO is responsible for the effective implementation of Vault's AML/KYC program. The officer oversees due diligence, transaction monitoring, and ensures that suspicious activities are reported to the relevant authorities.

10. Reporting

Vault is obligated to report any suspected money laundering, terrorist financing, or illegal activity to regulatory authorities without notifying the user. Unauthorized disclosure of such reporting is a criminal offense under applicable law.