AML COMPLIANCE NOTICE

Last updated on [_____] 2026 (Switzerland, version 1.0)

INTRODUCTION

Trustyfi Sàrl ("Trustyfi", "Company") maintains a strict stance against money laundering, financing of terrorism, and any other illicit activities. Trustyfi is dedicated to implementing an internal control system that includes policies, procedures, and controls that adhere to the highest industry standards and the most effective anti-money laundering and counter-terrorist financing (**"AML/CTF"**) measures. Established standards apply to all Trustyfi's Users and all persons associated with Trustyfi, including directors, staff members, contractors, and consultants, without any exceptions.

The objective of this Trustyfi AML Compliance Notice is to offer the Company's partners, clients, vendors, contractors, employees, regulators, law enforcement authorities, and other relevant stakeholders a high-level overview of the Company's AML/CTF compliance framework and its associated procedures (jointly referred to as the **"AML Compliance Notice"**). It's important to note that this Trustyfi AML Compliance Notice does not encompass the comprehensive set of policies, procedures, and controls established by the Company to prevent money laundering, the financing of terrorism, and other forms of illicit activities, and is provided for information purposes only.

Trustyfi is operated by Trustyfi Sàrl, a limited liability company (société à responsabilité limitée) incorporated under Swiss law, UID CHE-347.614.429, with its registered office at Rue de Carouge 28, 1205 Geneva, Switzerland. Trustyfi is a financial intermediary within the meaning of Art. 2(3) of the Swiss Federal Act on Combating Money Laundering and Terrorist Financing (AMLA, SR 955.0), affiliated with the self-regulatory organisation SO-FIT (Organisme de Surveillance pour Intermédiaires Financiers & Trustees, Geneva) under membership no. [_____]. SO-FIT is a self-regulatory organisation recognised by the Swiss Financial Market Supervisory Authority FINMA.

Being a financial intermediary, Trustyfi (i) is required to comply with the Swiss Federal Act on Combating Money Laundering and Terrorist Financing of 10 October 1997 (AMLA, SR 955.0), the Anti-Money Laundering Ordinance (AMLO, SR 955.01), the regulations of SO-FIT, the Swiss sanctions legislation (Embargo Act, SR 946.231, and its implementing ordinances) and, as international standards, the FATF Recommendations, and (ii) is obligated to establish effective internal procedures and mechanisms to counteract money laundering and terrorist financing ("ML/FT").

Capitalised terms not defined in this Trustyfi AML Compliance Notice shall have the meaning defined in Trustyfi's Terms of Service.

This Trustyfi AML Compliance Notice outlines:

- Tasks and obligations toward preventing money laundering and terrorist financing;
- Internal controls and procedures;
- User identity verification procedures;
- The role of the Company's Money Laundering Reporting Officer ("MLRO");
- Transactions monitoring and risk assessment;
- Reporting and record-keeping;
- Sanctions;
- Politically Exposed Persons**;**
- Restricted countries and territories.

TASKS AND OBLIGATIONS TOWARD PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

To detect and prevent money laundering and terrorist financing, Trustyfi performs the following tasks when performing its activities:

- Creates an assessment of the risk of money laundering and terrorist financing;
- Establishes policies, controls, and procedures to effectively mitigate and manage the risks of money laundering and terrorist financing;
- Implements measures to get to know the customer (customer review);
- Reports to the Money Laundering Reporting Office Switzerland (MROS) where required by Art. 9 AMLA, and blocks assets where required by Art. 10 AMLA;
- Appoints an AML officer (MLRO), who may be an external specialist mandated in accordance with the SO-FIT regulations, and ensures the conditions for his or her work;
- Takes care of regular professional training of employees and ensures regular internal control over the performance of tasks, and is subject to periodic AML audits by an external audit firm recognised by SO-FIT;
- Prepares a list of indicators for identifying customers and transactions concerning which there are reasons to suspect money laundering or terrorist financing;
- Ensures the protection and storage of data and manages the records prescribed by the law;
- Performs other tasks and obligations under the AMLA, the AMLO and the SO-FIT regulations.

TRUSTYFI'S INTERNAL CONTROLS AND PROCEDURES

Trustyfi has established and put into practice internal controls and procedures designed to efficiently address and handle risks associated with money laundering and terrorist financing. These risks are identified through a risk assessment aligned with Trustyfi's risk-based approach.

USER IDENTITY VERIFICATION

In accordance with the AMLA and the SO-FIT regulations, Trustyfi is obliged to verify the identity of its Users and to establish the identity of the beneficial owner and, for legal entities, of the controlling persons, prior to performing any transactions (Art. 3 and 4 AMLA). User identification is performed in the following cases:

- Establishing a business relationship with a User;
- In the case of any transaction, irrelevant to its value;
- Where there are doubts as to the authenticity and relevance of information previously obtained about the User or the beneficial owner of the User;
- Whenever there are grounds for suspecting money laundering or terrorist financing in relation to the transaction, the User, the funds, or the assets, irrespective of the value of the transaction;
- In other cases, subject to Trustyfi’s absolute discretion.

During the identification and verification process, Trustyfi may require the Users to provide supporting documents proving the information provided during the identification and verification process.

Trustyfi needs to unequivocally establish the User's true identity as a legitimate natural or legal entity. While Trustyfi may occasionally utilise third-party sources for fact-checking during User onboarding, Trustyfi holds full legal responsibility for ensuring the checks meet the required standards.

In some cases, for example, when the transaction amount exceeds Trustyfi’s internal limits, the User’s actions are suspicious, or their purpose is unclear, or the User’s risk level has increased, Trustyfi may, at its own discretion, ask the User to pass additional verification procedures and provide additional details or documents.

All User identification information will be collected, stored, shared, and safeguarded confidentially and in strict compliance with Trustyfi's Privacy Notice and the associated regulations in accordance with the Swiss Federal Act on Data Protection (FADP).

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

The MLRO is an appointed person responsible for implementing and performing the anti-money laundering and ‘Know Your Client’ (**“AML/KYC”**) procedures, transaction monitoring, mitigating ML/FT risks, and performing AML/CFT duties and obligations

of Trustyfi. MLRO is also responsible for staff training, reporting suspicious transactions to the authorities, and ensuring Trustyfi's overall compliance with applicable AML/CFT law.

Please do not hesitate to contact the MLRO in case of any ML/TF concerns connected with Trustyfi via: info@trustyfi.ch.

TRANSACTION MONITORING

Trustyfi constantly monitors the Users' accounts and transactions for suspicious activity, illegal transactions, or other issues. Trustyfi may employ higher or lower levels of scrutiny when monitoring the Users' transactions based on its risk assessment and risk appetite arrangements.

Based on the transaction monitoring, Trustyfi may perform additional checks, require additional information from the Users, and, in some cases, suspend any transactions and the provision of Services.

When transferring Crypto-assets, Trustyfi applies the information requirements for transfers of virtual assets applicable in Switzerland (Travel Rule) and verifies that the external wallets used by its Users belong to them. Each wallet and transaction is screened with blockchain analytics tools before execution.

RISK ASSESSMENT

Trustyfi applies a risk-based approach when performing the AML/KYC procedures to assess particular risks and attribute them to each of Trustyfi's Users. The risk-based approach uses several criteria, such as:

- Customer risk;
- Geographical risk;
- Product risk; and
- Delivery channel risk.

Risks are assessed and revised periodically. Based on the risk assessment results, Trustyfi may request further information or documents from the User, deny the provision of the Services, suspend access to the Platform, and take further actions according to the applicable law.

REPORTING AND RECORD-KEEPING

Under Art. 9 AMLA, Trustyfi is required to report without delay to the Money Laundering Reporting Office Switzerland (MROS) if it knows or has reasonable grounds to suspect that assets involved in a business relationship are connected with money laundering, derive from a felony or an aggravated tax misdemeanour, are subject to the power of disposal of a criminal or terrorist organisation, or serve the

financing of terrorism. Trustyfi may be required to block the assets concerned (Art. 10 AMLA) and is prohibited from informing the persons concerned or third parties of such a report (Art. 10a AMLA).

Under applicable law, Trustyfi is required to retain and provide to the responsible authorities certain documents and information about its Users and their transactions for at least 10 years after the termination of the business relationship or the completion of the transaction (Art. 7(3) AMLA). Such information will not be deleted at the Users' request.

SANCTIONS

Trustyfi is prohibited from transacting with persons, entities and bodies under international sanctions. Trustyfi screens all its Users against the lists of applicable sanctions, in particular the sanctions lists of the State Secretariat for Economic Affairs (SECO) under the Embargo Act, as well as UN, EU, UK and OFAC lists, as well as analyses the subject matter of transactions to ensure compliance with international sanctions. Any sanction screening match is escalated to the MLRO for further action. Trustyfi will not perform any transaction if it assumes or suspects that a risk of breaching applicable sanctions is associated with it.

POLITICALLY EXPOSED PERSONS (PEPs)

Trustyfi realises that, due to the possibility of abusing their public office for private gain, PEPs are required to be subject to enhanced scrutiny. Therefore, Trustyfi screens all its Users against the PEP lists at onboarding and on an ongoing basis. As a matter of risk policy, Trustyfi does not establish business relationships with PEPs, their family members, or close associates. Where a User is identified as a PEP, a family member or a close associate of a PEP in the course of the business relationship, Trustyfi will terminate the business relationship in compliance with its obligations under the AMLA.

RESTRICTED JURISDICTIONS

Trustyfi does not offer or provide its Services to individuals residing in or entities registered in countries and territories that:

- Have been identified by international organisations as having a high risk of money laundering;
- Have been sanctioned by the UN, the EU, Switzerland (SECO), or another body;
- Consider Trustyfi's services unlawful and have officially prohibited them;
- Other countries or territories Trustyfi deems high-risk or is not ready to provide services in for other reasons.

You may find a full list of restricted jurisdictions on our website.