Embily AML/KYC Policy

Version: 1.02

Last updated: September 10, 2020

1. Introduction

This Embily AML/KYC Policy (“ **Policy** ”) sets forth the rules and procedures that the btc2wire OÜ, a company incorporated under the laws of Estonia with a registered code **14915269** , its subsidiaries and affiliated parties (the " **Company** ") follows for detecting and preventing any financial crime.

This Policy is an integral part of the Company’s Terms of Use, which are at all times available on the Company’s website.

The Company is strongly committed to preventing the use of its Services for money laundering or any activity which facilitates money laundering, the funding of terrorist or criminal activities, or any other illicit purposes.

The Company follows internal AML/KYC procedures (the “ **Procedures** ”) for its Services, including virtual currency services, that together comprise the Company’s AML/KYC Program.

The Procedures are administered by the Company’s director, and/or the Compliance Officer, and his team, together referred to as the Compliance Department. The **Compliance Department** is tasked with monitoring compliance with the relevant AML/KYC regulations and administrating the Procedures within the Company.

2. AML/KYC Framework

The Company is licensed by the Estonian Financial Intelligence Unit (the “ **FIU** ”) to provide Services virtual currency services (FVT000024).

The Company administers AML/KYC measures and Procedures, required by the Estonian Money Laundering and Terrorist Financing Act (the “ **Act** ”) and other legal guidelines given by the Estonian Minister of Finance for businesses licenses to provide the Services.

3. Protection Measures

The Company has implemented protection measures, which protect the Company from being involved and the Company’s Users from carrying out any suspicious financial activity, by:

1) Performing KYC procedures on Users – natural and legal persons and their representatives;

2) Performing an enterprise-wide risk assessment to determine the risk profile of the Company;

3) Implementing internal procedures, policies, and controls aimed at mitigating risks of money laundering and terrorist financing;

4) Conducting AML/CTF staff training;

5) Conducting a periodic AML audit;

6) Maintaining and updating User information;

7) Reporting suspicious transactions to the relevant financial authority (the FIU).

4. KYC Measures

As part of the User Due Diligence, the Compliance Department shall:

1) Identify the User and/or its representative and verify submitted information using reliable, independent sources, including using means of e-identification;

2) Confirm the authenticity of documents and information provided by Users;

3) Investigate Users, whose activities and/or documents have been identified as suspicious or risky;

4) Request additional and/or updated documents and information from Users when deemed necessary by the Company at any time;

5) Verify Users' transactions on an on-going basis even if Users have been identified in the past.

Please note that the Company shall have the right to request additional and/or updated documents and/or information from any User at any time, even if such User has been identified before. The Company may stop providing Services to Users and/or report such Users to the FIU if they do not provide the Company with requested documents and/or information.

5. Verification Levels & Requested Information

The Company shall implement different KYC Verification Levels, which are available at the Company's website. Verification Levels constitute an integral part of this Policy.

Verification Levels perform the following functions:

1) Providing access to Services offered by the Company;

2) Increasing thresholds of Services, available to Users.

The level of verification, conducted on each User shall directly influence the amount of activities said User can perform during the course of using the Services.

Information and documents requested from Users (both natural and legal persons) are available on the Verification Levels page.

For the purposes of the Verification Levels, the following terms shall have the following meaning:

1) **Valid ID** shall mean any of the following:

– an identity card, digital identity card; – a foreign passport

2) **Proof of Residence** shall mean a utility bill, bank statement, credit card statement, insurance, or tax statement issued within the last 3 months. (optional, might be requested additionally)

When making a transaction or a series of linked transactions for a value of more than 15,000 EUR or equivalent in any fiat or virtual currency or **at any time requested by the Company**, a User may be asked to provide a **Proof of Funds**. A Proof of Funds shall mean any document that verified the source of User's wealth, e.g. letter from a lawyer/agreement for gifts, sale agreement for funds acquired from the sale of property, tenancy agreement for rental income, copies of company's accounts, bank statements for salary information, etc.

The Company may also send a User, for the purposes of the Verification Levels **or at any time decided by the Company**, an KYC/AML Questionnaire. A **KYC/AML Questionnaire** shall mean a series of questions and/or a video-call with the Compliance Department, aimed to identify the intent and the source of funds that are subject to User's transactions and activities and to rule out any illicit purpose.

6. Risk Factors & Risk Assessment

When carrying out initial and/or ongoing Procedures, the Company takes into consideration the following risk factors:

Risk Factor	Risk Characteristic
Geographical	1. Country of residence or nationality of the User is a country with a risk of money laundering higher than usual;
	2. The User is a resident or a citizen of the low-tax or tax-free country.
User	1. The User provides untruthful facts, including but not limited to: discrepancies in provided ID documents, fictitious person, stolen identity, counterfeited ID document, post box home address, pervious financial crime record, terrorist record, wanted person, etc.
	2. The User performs suspicious, high-volume, and unusual transactions;
	3. The User is a politically-exposed person.

The Company may apply simplified or enhanced AML/KYC measured (as defined in the Act), based on the results of the risk assessment.

List of countries and territories the Company does not work with: Afghanistan, Bahamas, Benin, Cameroon, Central African Rep, Chad, Congo (Democratic Republic), Cote D'Ivoire, Cuba, Eritrea, Gaza Strip, Ghana, Guinea, Guinea Bissau, Haiti, Iran, Iraq, Korea (Democratic Republic), Kuwait, Lebanon, Liberia, Libya, Mali, Myanmar (Burma), Nicaragua, Pakistan, Panama, Palestine, Qatar, Somalia, South Sudan, Sudan, Syrian Arab Republic, Togo, Trinidad & Tobago, Uganda, USA, Venezuela, West Bank, Yemen, Zimbabwe, Crimea, Luhansk National Republic (LNR), Donetsk National Republic (DNR), Nagorno Karabakh, Kashmir, Gaza Strip, West Bank, South Ossetia, Abkhazia

7. Monitoring Requirements

The Company carries out ongoing monitoring of activities to prevent money laundering, terrorism financing, and other illegal activities.

As part of the monitoring requirements, the Company shall:

1) Check transactions of its Users;

2) When needed, request documents to update/confirm information gathered when applying KYC measures;

3) When needed, identify the User's source of funds;

4) Pay additional attention to suspicious, high-volume, and unusual transactions;

5) Pay additional attention to transactions made by Users from countries with a risk of money laundering higher than usual.

8. Suspicious Activity Detection & Reporting

In an event that the Company suspects suspicious transactions, as identified in its internal policies and procedures, based on the FIU Guidelines , it shall conduct additional questioning regarding the User activity by the means of the KYC/AML Questionnaire, and request any additional documents and/or information that may be required.

In case the User has not provided document and/or information and explanation about the suspicious transaction, a complete set of requested documents, or has presented suspicious or unusual documents that the Company cannot verify, and the Company reasonably suspects that User's activities may be connected to money laundering, terrorism financing, or other illegal activities, the Company shall file a report on the FIU website reporting the suspicious activity and reserves the right to suspend the User's account, suspected of such activities at its sole discretion.

9. Contacting the Compliance Department

If you have any questions about this Policy, the Procedures, or any other AML/KYC-related matters, please contact the Compliance Department at: aml@btc2wire.eu