1. Our Mission: To Promote and Facilitate Access to Virtual Assets

This Anti-Money Laundering and Counter-Terrorism Financing Policy ("Policy") has been developed by BitHorizon LLC ("Company") and establishes the core principles and control mechanisms for preventing money laundering and terrorism financing ("ML/FT"). The Company aims to develop an Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") system and implement appropriate preventive measures to avoid the placement of illegally obtained funds into legitimate financial systems. To this end, the Company identifies, analyzes, manages, communicates, and mitigates risks.

BitHorizon LLC recognizes that fraud, money laundering, terrorism financing, and other financial crimes are harmful not only to individual customers but also to broader social and public interests, including national security, public order, and the personal and financial security of citizens. Combating such crimes requires a collective, organized, and coordinated effort from international organizations, governmental bodies, private sector entities, and individual citizens.

As practice has shown, the most effective method of fighting financial crime is early-stage prevention. In recent years, this approach has been recognized as a universal international standard.

BitHorizon LLC, as a company that sees its mission in promoting the dissemination of virtual assets, fully understands the threats posed by money laundering, terrorism financing, and similar crimes. It also recognizes that the widespread use of virtual assets must be accompanied by sector-specific measures—a "golden mean," if you will—that ensure the reliability and safe use of virtual assets by customers, without creating artificial barriers to access and free usage.

Consequently, BitHorizon LLC is committed to planning and delivering its services in a manner that aligns with international standards for combating money laundering and terrorism financing, while minimizing unnecessary obstacles for clients. It is important to emphasize that our primary goal is to prevent our products and software from being used for money laundering, terrorism financing, fraud, or related crimes.

In line with this approach, the Company has established a governance scheme, operational structure, employee team, and internal procedures to maximize the prevention of money laundering and terrorism financing. These efforts focus on addressing new challenges to AML compliance in an evolving financial environment, as well as developing and implementing the necessary technologies, software, and procedures.

The Company has assembled an AML/CFT compliance team composed of individuals with relevant knowledge and experience. Employees undergo periodic training to stay informed about the latest best practices and methods of combating financial crime and applying them in practice. The decisions of this team regarding issues related to money laundering and terrorism financing prevention are final and binding with respect to any client transaction.

The Company has implemented internal procedures to prevent the facilitation of money laundering and terrorism financing. These measures include:

2. Identifying Individuals

Registration on BitHorizon LLC's website is a mandatory prerequisite for receiving services. The first step of registration involves accurately determining the interested party's identity. BitHorizon LLC relies on the following data to identify individuals:

- Full Name
- Date of Birth
- Personal Number (if available)
- Identification or citizenship-validating document number, date of issue, issuing country, issuing authority, and validity period
- Gender
- Citizenship
- Place of Birth – country (and city, if available)
- Registered Address
- Actual Residential Address

3. Identifying Legal Entities

To register legal entities, clients must provide both the entity's registration data and identification data for individuals holding authority and for founders (including beneficial owners). To identify legal entities, BitHorizon LLC requires the following basic data:

- Name
- Registration Date
- Legal Address
- Identification Number (if available)
- Registration Number (if available)
- Legal Form
- Actual Location Address

Additionally, in the case of unregistered organizational formations, it is necessary to identify individuals with managerial and representative authority, as well as founders (including beneficial owners), using the following data:

- Full Name
- Date of Birth
- Personal Number (if available)
- Identification or citizenship-validating document number, date of issue, issuing country, issuing authority, and validity period
- Gender
- Citizenship
- Place of Birth – country (and city, if available)
- Registered Address
- Actual Residential Address

If the client is a branch of a legal entity, additional information must be provided about the parent company and its authorized individuals, using the same identification criteria listed above.

4. High- and Low-Risk Factors

The Financial Action Task Force (FATF) is an independent intergovernmental body that promotes policies to combat money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction. FATF has issued recommendations that are widely recognized as international standards in the fight against ML/FT. These standards include specific requirements for judicial bodies, financial intelligence units, law enforcement agencies, the private sector, and oversight authorities.

FATF's recommendations categorize risk factors as high or low. In cases of client identification, special attention should be given to circumstances that are unusual between parties in a business relationship or when the business structure itself is excessively complex or obscure.

5. Identifying Politically Exposed Persons

In accordance with international standards, a politically exposed person (PEP) is someone who holds a public or state position or is involved in significant political, public, or governmental activities. Enhanced client identification measures are applied when dealing with PEPs due to their potential influence, which may facilitate money laundering, terrorism financing, or corruption. When interacting with PEPs, their family members, or close associates, the Company takes reasonable measures to determine the source of funds and applies enhanced ongoing monitoring to the business relationship.

6. Identifying Clients from High-Risk Countries and Organizations

In accordance with Georgian legislation and BitHorizon LLC's internal policy, the Company will terminate or refuse a business relationship with any client who cannot be properly identified or who is listed as a terrorist or terrorism supporter. Furthermore, the Company categorically does not serve citizens or legal entities from high-risk jurisdictions or sanctioned countries, including the Russian Federation and the Republic of Belarus.

The decision to engage with clients from other sanctioned jurisdictions is made on a case-by-case basis, based on a comprehensive review of all relevant circumstances and assurances that the business relationship will not be used for money laundering or terrorism financing. Additionally, enhanced due diligence measures are implemented to determine the source of funds and monitor the relationship on an ongoing basis.

7. Know Your Customer (KYC)

BitHorizon LLC collects information about its customers through a Know Your Customer (KYC) questionnaire, which customers are required to complete. Until the questionnaire is fully and properly completed, customers will not have access to the full range of services offered by BitHorizon LLC.

To mitigate ML/FT risks, the Company identifies its clients in the following instances:

(i) upon the establishment of a business relationship; and
(ii) during single transactions.

The Company implements the KYC Standard:

(i) at intervals corresponding to the risk level assigned to the client; or
(ii) whenever there is a material change in the client's circumstances, regardless of the regular schedule.

The establishment or continuation of a business relationship is prohibited if the client cannot be properly identified, verified, or subjected to the required preventive measures.

Before entering into a business relationship, the Company verifies the identity of the individual client, the authorized representative (in the case of legal entities), and the beneficial owner against lists of sanctioned individuals and politically exposed persons using the AML Bot.

Confirmed by
BitHorizon LLC
Date: 2025