POLICY FOR THE PREVENTION AND COMBATING THE LAUNDERING OF DINHEIRO AND FINANCIAMENTO TO TERRORISM

Money laundering is understood to be the set of commercial or financial transactions that seeks to incorporate into the formal economy resources that originate from illegal acts, giving them legitimate appearance. The activities of raising, intermediation and applying own or third-party resources, in national or foreign currency, can be used in the practice of illegal financial transactions, which makes thefinancial systemparticularly vulnerable to money laundering.

The money laundering process involves three steps: placement, concealment and integration. Placement is the stage in which the criminal introduces the money obtained unlawfully into the economic systemthrough deposits, purchase of negotiable instruments or purchase of goods. It deals with the removal of money from the site that was illegally acquired and its inclusion, for example, to the financial market.

Concealment is the moment the agentperforms suspicious and characterizing the crime of laundering. At this stage, several complex transactions are configured to disassociate the illegal source of money.

In integration, the illegal resource definitely integrates the economic and financial system. Atthe time, the money receives a lawful appearance.

Terrorism in turn is characterized by the indiscriminate use of violence, physical or psychological, through attacks on people or facilities, with the aim of raising the feeling of fear insociety, disorganizing it and politically weakening governments or states for the takeover of power. It is used by a wide range of institutions as a way to achieve its objectives, such as political organizations, separatist groups and even governments inthe poder.

CHAPTER I - COVERAGE

All employees must adopt best practices when registering clients, transact assets on behalf of funds and/or portfolios under management and devote special attention to concepts and activities that help prevent and combat money laundering and terrorist financing.

CHAPTER II - OBJECTIVE

This Bitcoin To You Policy to Prevent and Combat Money Laundering and Terrorist Financing aims to:

- ✓ Establish and document The Policy Program for the Prevention and Combat of Money Laundering and Financial Terrorism ("Program") compatible with the size, volume of transactions, nature and complexity of Bitcoin To You products, services, activities, processes and systems;
- ✓ Identifypipelines, services and areas that may be vulnerable to money laundering activity, define activities and countries sensitive to money laundering, as well as identify atypical movements that may characterize the evidence of this crime.

CHAPTER III - LEGAL BASIS

The activities developed by BitcoinToYou are not specifically regulated. However, in September 2019 we had a first government regulation, which instituted ancillary obligations to exchanges, legal entities and individuals that transact cryptoassets. The importance of this advance is precisely to bring transparency and more solidity to operations with cryptoassets and consequently, even indirectly.

However, with a focus on Preventing Money Laundering and Combating Terrorism, BitcoinToYou adopts by analogy the following regulatory standards that deal with the prevention of money laundering and combating the financing of terrorism:

- Law 9.613 of March 3, 1998: typifies the crime of money laundering or concealment of assets, rights and values, and institutes measures that confer greater responsibility to the entities that make up the financial system, also creating within the scope of the Ministry of Finance, the Council for The Control of Activities Financeiras ("COAF").
- Circular No. 3,461, issued on July 24, 2009: consolidating the rules on the procedures to be adopted in the prevention and combating of activities related to crimes provided for in Law No. 9,613/1998.
- Law 12,846 of August1, 2013: provides for the administrative and civil liability of legal entities for the practice of acts against the public administration, national or foreign, and provides other measures;
- Circular Letter BC 3,542 issued on March 12, 2012: divulga list of operations and situations that may constitute indications of occurrence of money laundering crimes and combating terrorist financing. This circular letter repeals Circular Letter 2826/98.
- CVM Instruction 301, issued on April 16, 1999: provides for the identification, registration, registration, operations, communication, limits and administrative responsibility related to the crimes of "laundering" or concealment of assets, rights and values;
- Decree No. 8,420 of March 18, 2015: provides for the administrative responsibility of legal entities for the practice of acts against the public administration, national or foreign.

CHAPTER IV - POLITICALLY EXPOSED PERSONS

In accordance with CVM Instruction No. 463/08, Resolution COAF no. 16/07, Circular 3461/09 and Circular Letter 3430/10 of the Bacen, BitcoinToYou and its collaborators must pay special attention to politically exposed persons. It is considered to:

I – a person who has performed or has performed, in the last five (5) years, positions, jobs or relevant public functions, in Brazil or in other countries, territories and foreign dependencies, as well as their representatives, family members and other persons of their close relationship.
II – relevant office, employment or civil service exercised by heads of state and government, high-level politicians, high-level civil servants, high-level magistrates or military officials, leaders of public companies or political party leaders;ticos; e
III – relatives of the politically exposed person, his relatives, in the hotline, up to the first degree, as well as the spouse, partner and stepson.

Without prejudice to the definition of item I above, people in Brazil are considered politicallyexposed:

I - os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;
II - the occupants of office, in the Executive Power of the Union: a) minister of state or equivalent; (b) of a special or equivalent nature; c) of President, Vice-Presidentand Director, or equivalent, of municipalities, public foundations, public companies or mixed-economy companies; or d) of the group senior management and advisory - DAS, level 6, and equivalent;
III - the members of the National Council of Justice, the Supreme Federal Court and the higher courts;
IV - the members of the National Council of Public Prosecutions, the Attorney General of the Republic, the Deputy Attorney General of the Republic, the Attorney General of Labor, the Attorney General of Military Justice, the Deputy Attorneys General of the Republic and the AttorneyS General of the States and the Federal District;
V - the members of the Court of Auditors of the Union and the Attorney General of the Public Prosecutor's Office before the Court of Auditors of the Union; VI - theGovernors of State and the Federal District, the Presidents of the Court of Justice, the Legislative Assembly and the District Chamber and the Presidents of The Court and the Board of Auditors of States, Municipalities and the Federal District;
VII - the Mayorsand Mayors of City Council of state capitals.

In addition to the people described above, individuals who declare themselves politically exposed through their own field in bitcointoyou's Registration Form and those pointed to in public or private lists surveyed by Compliance.

CHAPTER V -DASTRO CUSTOMER CA

The registration of clients is an essential element in the prevention and fight against the crime of money laundering. BitcoinToYou's registration form is clear, objective and segregated in individuals and legal entities. All documentation must be carefully analysed for thepurpose of confirming the registration.

Compliance assesses the client's level of risk at the time of initial and reassessment analyses focusing on possible money laundering or terrorist financing practices,previously described. The results of the analyses allow the client to be adequately classified for monitoring, when any situation that allows monitoring of their movements is observed.

Thus, when classified formonitoring, it should also be classified according to the list below for monitoring and monitoring:

- PEP list
- Restrictive List
- Sanctions List
- Non-Resident
- Pointed out in the Anti-Corruption Act
- Pointed in Media
- Great Fortunes

Considering the main guidelines and rules existing in the financial market and cryptotrading, as well as the analysis of the main cases of money laundering, it is possible to relate the most sensitive people of involvement with the crime of money

laundering. All BitcoinToYou employees must devote attention to customers listed for monitoring and classified as above.

CHAPTER VI - EVIDENCE OF MONEY LAUNDERING

In accordance with the regulations mentioned above, it is of paramount importance that all trainees, employees, service providers, autonomous agents and partners are aware of the operations that constitute evidence of money laundering. The following are considered evidence of money laundering,operations:

- whose values appear objectively incompatible with the professional occupation and the declared financial situation;
- between the same parties or for the benefit of the same parties, in which gains or losses are followed with regardand to any of those involved;
- significant oscillation in relation to the volume and/or frequency of business of any of the parties involved;
- whose characteristics and/or developments evidence, in a blunt manner, on behalf of third parties;
- which evidence sudden and objectively unjustified change in relation to the operational modalities usually used by the involved);
- in order to generate loss or gain for which it objectively lacks economic foundation; and
- the degree of complexity and risk of which appear to be incompatible with the technical qualification of the client or his representative.

The following practices can also be configured as evidence of money laundering:

- create resistance in facilitating the information needed for the account;
- declare several bank accounts and/or modify them with usuality; And
- account and authorize a prosecutor who does not have an apparent link.

All interns, employees, service providers, autonomous agents and partners must report cases of suspected money laundering to compliance that will be responsible for

respecting the confidentiality of the report and providing proper investigation of the facts.

CHAPTER VII - ACTIONS AGAINSTMONEY LAUNDERING INDIVIDUALS

The routines defined by BitcoinToYou against evidence of money laundering aim to identify transactions with counterparty recidivism, unjustified or atypical transfers, operations with equity incompatibility, not limited.

A customer whose operations are atypical will be flagged and monitored, and also collected other information from this client such as:

- if you are politically exposed;
- if an atypical change of address or ownership of an account byearbook or attorney has been made;
- if you reside/have an account/proxy at border locations.

Once the occurrence is generated, it will be up to the Compliance to analyze the client more deeply to confirm or not the suspicion of evidence of money laundering. The analysis will consistof the verification of documents, movements and data confronted by the respective system.

There are several possible measures, among them: the requirement of cadastral updating, a request for clarification to the advisor, the client's commercial or theclient himself, analysis of the Risk department facing movement inconsistencies or the filing of the occurrence itself. Each will be used according to the case in question.

If after the other analyses the suspicion is confirmed, compliance shouldre-verify such system analyses in the client's history and prepare formal communication to the COAF. The Executive Committee on The Prevention and Combating Of Money Laundering and Financing of Terrorism will be involved in deliberating by communication to the COAF.

CAPÍTULTHE VIII - TRAINING

BitcoinToYou employees should be adequately trained in preventing money laundering and combating terrorist financing. To this aim, BitcoinToYou conducts periodic training stems from guiding members on the issue in question, as well as reinforcing the need to comply with the procedures set out in this document. The training will be applied when the employee admission to BitcoinToYou and in future opportunities such as form dandrecycling.

The trainings can be face-to-face or electronic (on line) and compliance can apply evaluations in order to test the knowledge of employees. The material used in the training addresses topics that are considered important according to current regulations, addresses concepts and procedures inherent in combating terrorist financing and encompasses the control and monitoring processes adopted by Bitcoin To You.

CHAPTER IX - FINAL CONSIDERATIONS

If proven to be non-compliance with the standards set forth herein, BitcoinToYou employees are subject to the following penalties:

- Warning
- Suspension
- Resignation

Additional questions and clarifications should be sent to the Compliance Coordinator.