Anti-Money Laundering and Sanction Policy

Written By	Agreed upon with	Date of development	Version
AML and Compliance Department	Management	05.09.2024	1.0

BITCREDIT

Contents

1. Purpose and Scope of the Policy

1.1. The purpose of the Anti-Money Laundering and Sanctions Policy (hereinafter - the Policy) developed by “Digital Platform” LLC (hereinafter - the Company) is to create an effective system for the prevention, detection and suppression of money laundering and terrorist financing (ML/TF) faced by the Company, which At the same time, ensure effective management of sanctions compliance risk.

1.2. The policy is based on the current legislation and regulatory norms, in particular: the Law of Georgia "On Facilitating the Suppression of Money Laundering and Terrorism Financing", as well as by-laws approved by the order of the head of the Financial Monitoring Service of Georgia, the orders issued by the President of the National Bank and other relevant normative acts.

1.3. The policy regulates the principles and rules of monitoring in order to facilitate the prevention of the legalization of illegal income and the prevention of terrorism financing, defines the characteristics of an effective control system, which in turn is based on a risk-based approach and ensures the identification of risk factors facing the company through the optimal allocation of the company's available resources, classifying them according to categories and carrying out proportional control mechanisms of identified risks.

2. Sanctions

2.1. The policy prohibits relationships or transactions involving sanctioned individuals and entities or sanctioned countries, territories and their governments. In accordance with the Company's regulatory requirements and internal policies, the Company may from time to time refuse to carry out a transaction, freeze assets or refuse to provide services. It also means that in some cases the risk appetite of

internal policies and sanctions may be more stringent than regulatory obligations and the Company may not support doing business with certain customers even if it is regulatory permitted.

2.2. The Company commits to comply with the requirements set by the National Bank of Georgia in accordance with the rules of execution of sanctions regimes..

2.3. The company verifies the customers, beneficial owners, authorized persons, business partners and third parties in the databases of sanctioned persons. As a mandatory, the company uses the following lists:

2.3.1. UN Sanctions Lists;

2.3.2. EU Sanctions Lists;

2.3.3. OFAC Sanctions Lists;

2.3.4. UK Sanctions Lists;

2.3.5. List of sanctioned persons defined by the Government of Georgia

3. Risk Based Approach

3.1. In order to adequately manage the monitoring process, the company uses a risk-based approach, which means identifying the risk factors facing the company through the optimal distribution of resources and implementing proportional control mechanisms for the identified risks. Within the scope of the risk-based approach, the company analyzes the risks related to the geographical area, products/services, their delivery channels and customer profile.

3.2. A risk-based approach is also applied at the organizational level, which involves periodic assessment and analysis of existing products, customers and geographic risk.

3.3. Before introducing new products and processes, they are assessed and appropriate control mechanisms are implemented to minimize risk.

4. KYC / Customer Identification

4.1. The company has implemented "Know Your Client" (KYC) standard, which involves full identification/verification of customer, including beneficial owners of legal entities, seeking information about the purpose and intended nature of business relations, as well as updating existing information with predetermined periodicity. The KYC standard is performed every time a person opens an e-wallet.

5. Prohibited Business Activities

5.1. It is prohibited to establish or continue business relations or carry out any transaction, in following cases:

5.1.1. For anonymous customers or those attempting to open accounts under an apparently fictitious name

5.1.2. For a shall bank

5.1.3. It is not possible to verify / update the identification data of the person

5.1.4. The person is included in the list of sanctioned persons

5.1.5. If a person conducts transactions through a company that there is a reasonable suspicion that they were entered into or carried out for the purpose of money laundering

5.1.6. If the person turned out to be a politically exposed person and there is a written refusal from the company's management regarding relationship establishment

5.1.7. If the company's management refuses to provide services to a high-risk client

5.1.8. Upon receipt of FMS instruction on suspension of transaction execution

6. Transaction Monitoring

6.1. In accordance with the requirements of the Law of Georgia on the Facilitating the Suppression of Money Laundering and Terrorism Financing the Company monitors transactions and identifies mandatory reporting transactions and suspicious transactions.

6.2. Identification of transactions subject to mandatory reporting is carried out by an automated process and is being sent to the Financial Monitoring Service.

6.3. For suspicious transaction detection a Red Flags are used, which may indicate to money laundering or raise suspicions that the source of income is from an illegal activities or the transaction may be directed to the benefit of sanctioned persons or aimed at evading sanctions. In case of reasonable suspicion, the information is sent to the Financial Monitoring Service.

7. Record Keeping

7.1. Effective management of the monitoring process largely depends on the proper recording of information and its systematization in documented and electronic

form. Accounting of information about clients and their transactions is carried out in a specialized program.

7.2. All documents obtained during the identification of a person, as well as information and records about his accounts and carried out transactions, as well as other documents are stored for at least 5 years.

8. AML/Sanction program Audit

8.1. Audits of AML and sanctions-related processes are performed at least annually, which is carried out by the company's internal audit department.

8.2. The Company may conduct an assessment of its AML and sanctions related policies/procedures and process through an independent external auditor. At a minimum, such assessment should include internal documentation related to AML and sanctions, employee training, adequacy of AML and sanctions procedures, and automated monitoring systems.

9. Employee Selection and Training

9.1. Each employee of the company has an important role in performing the main functions of the company, therefore there is an expectation that he/she will be honest and competent towards the company in his work. An integral part of the employee selection process is the verification of potential candidates in the list of sanctioned persons.

9.2. All employees of the company, within their competence, are properly informed to be able to detect transactions with ML/TF signs. All employees must familiarize

themselves with the requirements of this policy and, if necessary, obtain additional clarifications.

9.3. The training program developed by the company is based on the ML/FT risk factors facing the company and the specifics of the employees' activities. Upon starting work, a new employee of the company must undergo an initial training, where they will be informed of the basic principles and mandatory requirements of AML/CFT. After initial training, all employees undergo regular training to improve their knowledge and keep up to date with changes in the field of money laundering and terrorism financing.

9.4. Periodic training of the employee is carried out at least once a year.

10. Reporting

10.1. The AML and Compliance Department ensures the creation of a compliance report and its submission to the Director. This report covers issues related to money laundering and sanctions - key risks, important news and incidents during the reporting period.

10.2. The report is submitted to the director semi-annually.

11. Confidentiality

11.1. The employees of the company are obliged to protect the confidentiality of the information at their disposal, in particular, not to disclose the existing information about the records, accounting files, business correspondence and the results of the conducted analysis in the company.

11.2. The information about considering this or that transaction as suspicious and the transfer of information to the financial monitoring service, as well as the measures related to the suspension of the execution of the transaction, are also confidential. Other than the head of AML and compliance and director, such information should be closed to all other employees of the company.

11.3. For breach of confidentiality, the employee shall be liable for disciplinary action and/or shall be held materially responsible for the resulting damages.