

Noflead N.V.

Anti-Money Laundering (AML) Policy

Version 2

**Drafted by Legal Department
Approved by Director, Besik Khokerashvili
Approval date 24-05-2018**

Clause

- 1. Preamble 3**
- 2. Definition of Terms 3**

- 3. Inner Control System 5**
- 4. Internal Policies and Procedures 5**
- 5. Monitoring Staff Members 6**
- 6. Risk-Based Approach 6**

- 7. Procedure Know Your Client 7**
 - 7.1 Identification of the Clients 7**
 - 7.2 Standard Measures of Identification 7**

 - 7.3. Termination of Business Relationship 8**
- 8. Data Stores and Data Register 8**
- 9. Report 9**
- 10. Selection of the Cooperators and Training 9**
- 11. New Products and Services Approval 10**
- 12. Anti-Bribery Policy 10**

1. Preamble

Noflead N.V. (hereinafter – Organization) represents the organizer of gambling business and owner of gambling business license, having been operating since 2018 and provides service on the online gaming website <http://noflead.com/> (hereinafter “Product”) organized within the frames of the gaming license.

With the purpose of ensuring the highest standards of the offered service and complete fulfillment of requirements of Law of Georgia, the Organization has elaborated the given policy “On Anti-Money-Laundering Control” (hereinafter “Policy”), based on: the Law of Georgia “On Facilitating the Prevention of Illicit Income Legalization”, provision of Financial Monitoring Service of Georgia “On receiving, systematization, processing information by Tax Service Provider and the rule of submitting such information to FMS of Georgia” and recommendations of Financial Action Task Force (FATF). The goal of the Policy is to elaborate identification of risks, analyses, conduct, reduce and control system for the Organization against money laundering and terrorism financing.

The Policy is confirmed by head of Organization and is subject to annual renovation.

2. Definition of Terms

Money Laundering – Making illicit income appear legitimate (acquisition, use, transfer and other action), and the hiding or concealment of its true origin, or its owner or possessor, and/or property rights, or the attempt thereof;

Terrorism Financing – any transaction (regardless the amount) implemented by any entity using any remedy whether directly or indirectly, illicitly and purposely, whose aim is to gain or collect monetary fund with the aim or, on the basis of the information that such amount is partially or wholly used for preparation or conduct of terrorist acts. In certain cases this may also apply to the legally gained assets.

Illicit Income - illegal and/or undocumented property owned or possessed by a person;

Property – All items (real estate, as well as movable property) and intangible property benefits that can be used owned and disposed by legal entities and individuals;

Identification - obtaining such information on a person that, where necessary, allows for investigating a person or for distinguishing a person from the others;

Client – An individual, who registers on the website as a service receiver (player).

Business Relationship – Relationship with the client based on the contract, which directly relates to receiving non-single-use service. Under such policy, opening an account on the website for the client, filling the balance, participating in gaming (placing bets, getting winnings), cash-out are deemed as business relationship.

Politically Exposed Person – a foreign citizen who occupies a state (public) political position and/or carries out important public and political activities under the legislation of the country. Politically exposed persons are: the Head of the State, the Head of the Government and Government members, and their deputies, heads of governmental institutions, Members of Parliament, members of the Supreme Court, members of the Constitutional Court, senior officials of the military forces, members of the Central (National) Bank / Financial Supervision Agency Council, ambassadors, heads of enterprises operating with state participation, heads of political parties (associations), members of the executive body of a political party (association), other significant political figures, and their family members and close associates; a person shall be considered as a politically exposed person for one year after his/her resignation from the above positions;

Suspicious Transaction – a transaction (irrespective of the amount and type of the transaction), with regard to which there are reasonable grounds for suspecting that the transaction has been entered into or conducted for the purpose of illicit income legalization and/or that property (including funds), based on which the transaction has been entered into or conducted for financial terrorism (a party to the transaction or the origin of the transaction amount is suspicious, or there are other grounds for which the transaction may be considered suspicious), or that any party to the transaction is included in the list of terrorists or there are other grounds for which the transaction may be considered suspicious), or that any party to the transaction is included in the list of terrorists or persons supporting terrorism and/or may be related to them, and/or the amount involved in the transaction may be related to or used for terrorism, terrorist acts, or by terrorists or terrorist organizations or by entities financing terrorism, or that the legal or actual address or place of residence of a party to the transaction is within a non-cooperative area, or that the transaction amount is transferred to or from a non-cooperative area;

Unusual Transaction - an unusually large, complex transaction (operation) and/or the unusual constituent parts of a transaction (operation) with no clear economic (commercial) content or clear legitimate purpose and/or those that are inconsistent with the ordinary course of activities of a party to the transaction;

Division of Transactions - under the given policy, means the unity of the implemented transactions, carried out by a person or in favor of a person during certain period of time,

the total amount of which exceeds 30 000 GEL or its equivalent in different rate and with regard to which there is reasonable ground for suspecting that they were divided deliberately with the aim to prevent sending report on transaction. The analysis conducted by monitoring staff member, represents the ground for substantiating the doubt.

Monitoring Staff Member – The employee designated on the ground of the Resolution, properly drafted by the Organization, who is liable for anti-money laundering coordination within the Organization.

3. Inner Control System

With the aim to prevent financing of Money laundering and terrorism, the Organization ensures creation of effective inner control system consisting of the following components:

- Internal policies and procedures

- Monitoring Staff Members

- Risk-based approach

 - Procedure “Know Your

 - Client” Data stores and

 - data register Report

 - Selection of the cooperators and training

 - New products and services approval

4. Internal Policies and Procedures

The given policy is the basis for the internal control of the Organization, which determines the main control mechanisms, responsibilities and principles for money laundering and terrorist financing prevention.

The procedure “Know Your Client” represents an integral part of the Policy, where the description of monitoring processes of the Client identification, verification and business relationship is provided.

The given Policy determines the criteria of granting risks to the Organization products and the Clients, and corresponding risk measures for the clients’ identification and verification. The given policy is available for all employees of the Organization.

5. Monitoring Staff Members

On the basis of properly drafted Resolution, the Organization assigns the cooperator (hereinafter – Responsible Cooperator) responsible for Anti-Money Laundering.

The Responsible Cooperator has to create and manage internal control system determined under the given Policy. In order to fulfill this function effectively, the Organization must make all the resources available for the Responsible Cooperator, such as: appropriate technical and software facilities with the function of storing information and documents safely etc.

Alongside with the Responsible Cooperator, it is the Organization's official's liability to ensure effectiveness of Anti-money Laundering System. Above all, those cooperators, who indirectly participate within the process of establishing business relations with the clients, are liable for inculcating separate control mechanisms.

6. Risk-Based Approach

Risk-based approach stands for the main principle of Anti-Money Laundering within the Organization, according to which the Organization differentiates its Products and Clients into low, medium and high risk categories. The identification and assessment of relevant risk-factors for financing of Money Laundering and Terrorism by the Organization represents the grounds of risk specification.

Specification of proper control mechanisms for medium and high risk category products represents the goal for identification and assessment of risk-factors, on the grounds of which it will be possible to reduce and manage the current risks, threatening the Organization, of Money Laundering and Terrorism.

7. Procedure “Know Your Client”

7.1. Identification of the Clients

Identification and verification of the clients represents one of the most significant control mechanisms for reduction of risks of financing Money Laundering and Terrorism. Taking into account the approach based on the risk, the intensity of verification measures depend on the specific risk category, which the client belongs to.

The Organization identifies the Client and takes reasonable measures for verification prior to making the deal or within the process of building business relationship.

7.2. Standard Measures of Identification

Standard measures of identification are used for low and medium-risk clients. According to the given procedure, the Client has to provide the following necessary documentation at the moment of making a deal or building business relations:

- ID card of a Georgian citizen;
- Passport of a Georgian citizen;
- Passport of a foreign country’s citizen;

The document confirming the entity’s identity must meet the following requirements:

- Must include requisites specific to such type of document (number, date of issue and validity, protective attributes etc.);**
- Must include passport holder’s photo;**
 - Photo must enable affirmation of the authentication with the document holder; Must be valid**
- Must not be substantially damaged.**

In case of necessity (for instance, if there is a doubt with regard to accuracy and/or correspondence of Identity details of the current clients), the entity, responsible for

monitoring, requires documents and/or any other information on transaction (operation) and its participants.

As a result of identification procedure of the Client, the following data should be indicated:

Full name;

Nationality;

Date and place of birth;

Place of residence;

ID (passport) number and personal number of the citizen according to the ID card (Passport);

7.3. Termination of Business Relation

The Organization refuses to build any business relations with the Client, or considers termination of current business relationship in following cases:

Client acts strangely;

The terms of the Agreement are violated from the Client's side;

The Organization has reasonable grounds to believe that the Client is involved in Money Laundering and fraudulent transactions;

In other cases – in accordance with the decision of the Responsible Individual.

8. Data Stores and Date Register

The Organization registers and stores the following type of recordings and documentations:

**Requisites, documents and/or their copies provided for identification of the Client;
Information on transaction (operation) (if applicable), as well as in the form of
electronic recording;**

Reporting presented to FMS of Georgia, both electronic and print versions.

The Organization ensures storing other evidences in relation to all recordings, documents and transactions listed above for the terms of at least three years since implementation of transaction.

9. Report

The monitoring of transactions, carried out by the Clients and sending reporting on appropriate transactions to Financial Monitoring Service of Georgia (hereinafter “FMS of Georgia”), is the most significant part of the Organization. The following transactions subject to sending reporting to FMS of Georgia:

If the total amount of transaction, or transactions, implemented for the purpose of its division, exceeds 30 000 GEL since the moment of implementation of transaction or not later than 5 business days since receiving the information on existence of such transaction or total transactions;

If transaction or identity details are deemed suspicious – since the day when such presumption or doubt was originated;

The Responsible Cooperator shall immediately investigate doubtful, unusual and noteworthy cases. If there is any reasonable doubt with regard to legality of origination of money, used in transaction and business relationship or with regard to reputation of the participant, reporting on suspicious transactions shall be immediately provided to FMS of Georgia. Detailed indications for identifying financing of Money Laundering and Terrorism are given in the procedure “Know Your Client”.

10. Selection of the Cooperator and Training

The Organization takes reinforced measures of identification when hiring the new employees. The significant attention is paid to reputation, qualification and respectability of the candidates for hiring them.

Face-to-face training should be held for all the employees of the Organization, who participate within the process of building business relationship with the clients within the terms of one month and afterwards – restudy training annually.

The Responsible Cooperator of the Organization shall participate in training for the purpose to increase knowledge and professional skills at least annually. Training should be of an appropriate quality in order to increase his awareness concerning liabilities under the relevant Regulation.

11. New Products and Services Approval

In case the Organization creates new Product or Services for the clients or significantly changes the specifics of the existing products and services, it should assess Money Laundering risk prior to inculcation of innovations and changes. The Responsible Cooperator participates in the process of risk assessment related to the new products/services, whose recommendations should be taken into account before final affirmation of the product/service design.

Money Laundering risks assessment is mandatory, even when segmentation of the service as well as using mediator organizations for managing the processes are considered.

12. Anti-Bribery Policy

Basic anti-bribery policy goals are:

- a) Determination of general policy of combating corruption;
- b) Elaboration of anti-bribery strategy and plan of actions for its implementation, periodic renovation, progress monitoring and assessment;
- c) Taking into account recommendations of relevant state bodies with regard to elaboration and implementation process of anti-bribery strategy and plan of actions for its implementation.

Elaboration of Anti-Bribery Plan:

It is necessary to underline strategic, operative and tactical management levels within the system of combating corruption. Each and every official will be liable for holding anti-bribery events and planning relevant management activity.

Attracting workers with relevant skills, giving trainings for the current workers, and ensuring their work process technically and in other ways plays a vital role in anti-bribery strategy success.

Preventive Measures

Structural and staff optimization of the establishments must be necessarily done, statement of duties of an employee must be elaborated and vividly stated; It should involve principles for both specification-distribution of responsibility and supervisor's control; for that purpose:

Ensure awareness of implementation of anti-bribery programs, giving skills development classes to the employees, taking decisions based on the true information and obtaining culture of execution oriented to work product and developing culture of relationship with the citizens, for that purpose:

- a) Mandatory (willful may also take place) workshops and trainings should also be periodically held for the employees;
- b) Typical thematic planning for raising qualification and training modules should be prepared;
- c) The principles of information availability, benevolent attitude and assistance, skill in error correction should be inculcated at workplace.

The employees must be necessarily stimulated in order to prevent temptation with regard to temptation that implies wage increase of the employees. Above all, the opportunity of a firm career development also plays significant role at the workplace.