

# **Anti-Money Laundering (AML) and Know-Your-Customer (KYC) Policy**

**Topc B.V. (reg. No. 163568)**

## 1. INTRO

**Topc B.V.**, the company registered in Curaçao, with its company number 163568, with registered office at Korporaalweg 10, Curacao (hereinafter to be referred to as “**Company**”, “**we**”, “**us**”, “**our**”) has developed this Anti-Money Laundering and Know-Your-Customer Policy (the “**Policy**”) in order to prevent money laundering, terrorist financing, and other illegal or fraudulent activity that may be conducted utilizing the services of the Company.

This Policy is applicable to internal (like employees and contractors) and external (clients) parties.

## 2. LEGAL GROUND

This Policy has been created subject to the following laws, regulations, recommendations, guidelines, and rules:

- a. The provisions of Curacao’s legal framework, which include, but are not limited to:
  - Lands Decree of the 7th November 2017, no. 2017/3297 establishing the consolidated text of the National Ordinance on the Reporting of Unusual Transactions (“**NORUT**”).
  - The National Ordinance of 23rd November 2015 amending the National Ordinance Identification of Client when Rendering Services (“**NOIS**”).
  - The National Ordinance Penalization of Money Laundering (“**NOPML**”), all as amended and updated.
  - Other applicable regulation
- b. The Regulations and Guidelines of the Financial Action Task Force (FATF):
  - International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (the FATF recommendations);
  - FATF Guidance on the RBA for Casinos.
- c. The legal framework of the European Union (to the extent applicable), which includes, but not limited to:
  - Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and supplementing Commission Delegated Regulations

## 3. PRINCIPLES OF THE POLICY

The Company employs the following principles to manage risks related to money laundering and terrorism financing:

- Conducting customer due diligence procedures, which includes enhanced measures for high-risk cases
- Adopting a Risk Based Approach (RBA) to evaluate ML/TF risks
- Implementing risk-based systems and procedures to monitor customers' ongoing activity
- Reporting suspicious activity internally and externally to relevant law enforcement authorities
- Maintaining records, including those related to internal investigations and external reporting, for the required minimum periods
- Providing training and screening to relevant employees and keeping them informed of the latest AML/CTF legislation to ensure their awareness is always sufficient.

#### **4. MONEY LAUNDERING AND TERRORISM FINANCING**

For the purposes of this Policy, “money laundering” means as any intentional conduct that aims to conceal or disguise the nature, source, location, disposition, movement or ownership of the proceeds of a crime or property derived from an unlawful act, with the intention of using it in a legitimate or illegitimate way, or to assist any person who is involved in a crime to evade the legal consequences of their actions. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another country.

In turn, “terrorist financing” can be defined as providing, collecting or receiving of funds, whether directly or indirectly, with the intention that they be used, or in the knowledge that they will be used, in full or in part, to carry out terrorist acts. A terrorist act is defined as any act that involves the use of violence or threat of violence, or any other form of intimidation or coercion, for the purpose of advancing a political, religious or ideological cause, and that is likely to cause death, serious bodily injury or significant damage to property.

#### **5. CORE MEASURES OF AML-CFT PROGRAM OF THE COMPANY**

The Company`s AML and CFT consists of the following measures:

- **Customer Due Diligence:** Company performs due diligence checks on all customers, including identity verification and screening against relevant AML databases. This includes enhanced due diligences measures as well.
- **Suspicious Transaction/Activity Monitoring and Reporting:** Company monitor transactions for suspicious activity and report any suspicious transactions to the relevant authorities.
- **Record Keeping:** Company must keep records of all transactions and customer due diligence checks for at least 5 years.
- **AML Training:** Company must ensure that all employees are trained on AML regulations and how to identify and report suspicious activity.
- **Risk Assessment:** Company conducts periodic risk assessments to identify and mitigate potential AML risks in their operations.

## 6. RISK BASED APPROACH AS A CORNERSTONE OF THE POLICY

The Company, being limited in resources and recognizing that money laundering/terrorist financing (ML/TF) practices continue to evolve, has adopted a risk-based approach (RBA) methodology. This methodology enables the Company to focus its anti-money laundering/combating the financing of terrorism (AML/CFT) measures on the areas/sections that pose the highest risk of ML/TF. The risk level of each customer is assessed when establishing a business relationship and continuously monitored throughout the relationship. The risk level of a customer may be adjusted at any time based on their activities.

For these purposes, the main risk areas that are considered by the Company are as follows:

- a. The country/geographical risk.** The country (or place) of the customer's residence (jurisdiction) is evaluated on the following criteria:
  - Whether the country of the customer's residence is specified in the list of "high-risk third countries with strategic deficiencies" of the Commission Delegated Regulation (EU) 2016/1675 and amending Delegated Regulations;
  - Whether the country of customer's residence is specified in the list of "high-risk and other monitored jurisdictions" of the FATF;
  - Whether the country of the customer's residence identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);

- Whether the country of the customer's residence identified as sanctioned by the OFAC;
- Additionally, the Company implements its own list of high-risk countries (national risk assessment). The following factors are taken into consideration when creating the national risk assessment:
  - The legal system (the presence of independent legal institutions, rule of law etc.);
  - Political environment and political stability;
  - Cultural background;
  - Geopolitical factors;
  - The crime rate in a particular country.

The Company explicitly sets geo-blocking measures (restriction to use/enter the websites on a software/hardware level) where the Company believes this is required or such jurisdictions are recommended to be blocked by legislative acts or recommendations of interstate bodies that set the standards in this field. For the avoidance of doubt, geo-blocking measures apply to the countries prohibited by licensing conditions in Curacao, namely USA, Netherlands, France, Dutch West Indies and Curacao as well as any other countries which might be communicated by the master licensor.

The Company performs clients checking against the list of sanctioned/non-serviced countries: Afghanistan, Central African Republic, Belarus, Ethiopia, Iran, Iraq, Israel, North Korea (the Democratic People's Republic of Korea), Donetsk Region, Kosovo, Latvia, Lithuania, Libya, Somalia, South Sudan, Sudan, Syria, Yemen, USA, Georgia, Russia.

**b. Customer behavior (customer) risk.** The Company conducts checks to identify any suspicious behavior of each customer. Suspicious behavior may include, but is not limited to:

- High spending amounts in comparison to the jurisdiction of the customer
- Use of multiple devices to log into the website in a short time frame or use of the same device or IP address by different customers
- Uncooperative behavior during the Customer Due Diligence (CDD) process, such as being defensive
- Unnecessary queries about withdrawals, including withdrawals to third parties
- Attempts by a customer to register multiple accounts with the website or with different websites operated by the Company
- Deposits that significantly exceed the usual gambling pattern of a customer

- Depositing a large amount but placing no or small bets, followed by a request to withdraw all funds
- Frequent deposits and withdrawals without any reasonable explanation
- Significant changes in the customer's gaming patterns (depositing, wagering, or withdrawal behavior, etc.)
- Transactions that appear disproportionate to the customer's wealth, income, or financial situation, etc. The Company is vigilant in identifying such behavior to prevent money laundering or terrorist financing.

The Company conducts constant monitoring of the activity of its customers to identify any of the risks, mentioned above and, if any, conducts standard or enhanced CDD measures to prevent any risk of money laundering, terrorist financing, or illegal activity.

Additionally, customers are screened for collusion with databases of the sanctioned persons, and such customers are not allowed to use the services of the Company.

## **7. CUSTOMERS DUE DILIGENCE**

Once the customer register on the Company's website, the latter performs initial CDD measures such as initial identification (collection of a series of personal details on the customer). Once identified, the customer is subject to ongoing monitoring of their activity.

If one of the triggers is revealed (both at the identification stage and later), the Company, depending on the nature and degree of risk's trigger, proceeds with either standard measures (like verification) or enhanced measures (advanced identification and verification including a stringent check of the source of funds and the source of wealth).

### **7.1. INITIAL CUSTOMER IDENTIFICATION**

Identification is the collection of information required to establish a customer's identity. Typically, a customer is identified by completing a registration form on a Company's website, indicating the following information:

- a. full name;
- b. date of birth;
- c. place of residence or seat / residential address.
- d. Contact email or phone number

### **7.2. STANDARD CDD MEASURES FOLLOWING IDENTIFICATION**

Standard CDD means verification of the players based on reliable documents.

For these purposes, the following documents and data could be requested from a customer:

- a. A copy or a photo of the identification document of the customer;
- b. A photo of the customer bearing his/her identification document and payment card;
- c. If applicable - customer's address confirmation. It may be a utility bill, telephone bill, or other documents, which, in accordance with the customer's jurisdiction legal and regulatory requirements, shall be enough to confirm the address of the customer;
- d. Photo of the customer holding a piece of paper with the requested information written by hand (the e-mail address of the customer, used when registering an account; the date of the photo request and the confirmation code).

The Company applies standard customer due diligence (CDD) in the following circumstances:

- a. The total amount of the transactions (deposit or withdrawal) made through the website by a customer reaches or exceeds NAF 4000 (EUR 2000) as a signal transaction or collectively from several transactions for one player. The Company reserves the right to carry out standards CDD regardless of reaching transactions' threshold, for example upon first withdrawal (meaning that the Company may conduct verification at the earliest convenience).
- b. A customer falls within one or more risk categories specified in the "Risk Based Approach" section above.
- c. When, in view of the situation, at the sole discretion of the Company CDD measures are deemed necessary;
- d. When there are doubts about the veracity or adequacy of previously obtained customer's information.

### **7.3. ENHANCED CDD MEASURES**

The Company conducts enhance customer due diligence measures when such measures are required by law, or Company believes that such measures must be applied in order to establish the absence of illegal activity of the customer. Such measures may be applied when:

- a. The customer is a Politically Exposed Persons in the meaning of Article 3(9) of the Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering

or terrorist financing or the customer is the member of the family of the Politically Exposed Person.

Under Article 3(9) of the abovementioned Directive, the Politically Exposed Person is a natural person who is or who has been entrusted with prominent public functions and includes the following:

- heads of State, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises.
- directors, deputy directors and members of the board or equivalent function of an international organisation.

The Company might use different databases in order to inspect whether a customer is a Politically Exposed Person or use services of third party providers to this end.

- b. The country of customer's residence is specified in the list of "high-risk third countries with strategic deficiencies" of the Commission Delegated Regulation (EU) 2016/1675 and amending Delegated Regulations;
- c. The country of customer's residence is specified in the list of "high-risk and other monitored jurisdictions" of the FATF;
- d. The legal entity or personal data of the client is listed in the United Nations Security Council Consolidated List
- e. Whether the country of the customer's residence identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- f. Whether the country of the customer's residence identified as sanctioned by the OFAC;.

In addition to the standard Customer Due Diligence (CDD) measures, Enhanced Due Diligence (EDD) could be applied to the above customers. The EDD measures include:

- a. The customer could be required to provide documentation on the source of wealth and funds used to make deposits on the website.
- b. The customer's identity will be checked using open registers, social media, and other publicly accessible sources to verify the information provided by the customer.
- c. In some cases, the customer could be asked to pass an interview through the video-call with a staff of the Company in order to establish that the account is really operated by the person specified in the documents submitted during the CDD. Generally, the Company uses Skype in order to conduct video-calls. Nevertheless, when the situation may require, other telecommunications software may be used.
- d. A photo of the payment card used (if a card is used) or intended to be used in making transactions on the website could be requested. It is important, that the name of the cardholder must be the same that the name of the customer that passes a verification. CVV code, and payment card number (except for the first 6 and last 4 digits) may be hidden or covered. The cardholder's name must not be hidden or covered in any manner;
- e. Senior management approval will be required before opening an account for a customer or continuing to operate an existing account.
- f. The Company will maintain ongoing, heightened control over the customer's relationship with the Company.

#### **7.4. ONGOING MONITORING**

The Company monitors customers' activities for suspicious behavior on an ongoing basis, including using different payment methods or cards, getting error codes when making payments, and using payment cards issued by different issuers in different regions. Customers who refuse to verify their account or payment instrument, or those with mismatched geolocation information, may also be flagged. Transactions are also monitored to ensure compliance with certain conditions, such as using a payment card with the same name as the account owner and not withdrawing funds to another customer's payment instrument.

**Suspicious Activity Monitoring.** All operations of customers are checked for the absence of suspicious activity on an ongoing basis. Suspicious activity includes, but is not limited to, the following:

- a. using multiple cards from different payment agents,
- b. encountering specific error codes during payment,

- c. using cards issued by different emitters in different regions,
- d. using different payment instruments in a short period,
- e. being unwilling to verify account or payment information,
- f. inconsistencies in customer geolocation data,
- g. refusal to participate in phone or video calls and provide photo identification,
- h. matching device IDs with another account in the system etc.

**Transaction Monitoring.** All the transactions of customers on withdrawal and deposits shall comply with the following conditions:

- i. If the transaction is made by using a payment card, the name of the holder shall be the same as the name of the website account owner. It means that any use of third-party payment card is prohibited;
- j. If the transaction is made by using an electronic wallet, this wallet's electronic mail may be the same that was used by a customer when registering an account on the Website;
- k. In case if a deposit is made from the payment instrument placement of funds to which is unavailable, the withdrawal shall be made to the customer's banking account or another payment instrument if it is possible to reliably ascertain that this payment instrument belongs to the customer in question;
- l. The Company does not withdraw funds that were deposited by the customer to the payment instrument of another customer.

## **8. REPORTING**

The Company submits reports to Curacao's Financial Intelligence Unit ("FIU") if the following indicator is in place:

- a. Objective indicators:
  - A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
  - An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
  - A transaction amounting to NAF (ANG) 5,000.00 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner, covering:
    - A giro-based transaction amounting to NAF (ANG) 5,000.00 or more;

- The taking into a deposit or the releasing out of the deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.
  - Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more.
  - Payout of prizes in the amount of NAF (ANG) 5.000 or more.
  - All other cases
- b. Subjective indicator:
- A transaction giving cause to assume that it may be connected with money laundering or terrorist financing which may include, inter alia:
    - The customer refuses to pass the Verification, and the Company has ample grounds to suppose that such a customer presents a risk of money laundering or terrorist financing.
    - The customer`s transaction(s) or activity is suspicious (as mentioned above).
- c. Additional indicators – any transaction with regard to which we suspect and have grounds to suspect that it:
- involves funds derived from illegal activities;
  - is intended to evade taxes or other legal obligations;
  - is designed to avoid the reporting or other requirements under the gambling legislation;
  - has no apparent economic or lawful purpose;
  - involves the use of false or forged documents;
  - involves unusual patterns of transactions that have no apparent economic or lawful purpose;
  - involves the use of an account in a fictitious name;
  - involves the use of an account that is held by someone other than the person conducting the transaction;
  - is conducted in a manner that is inconsistent with the customer's known or declared business or financial profile.

The Company submits reports to FIU via the online reporting system goAML.

Company understands and adheres to the restriction on the tipping off practices. In case the report is filled with FIU or any internal investigation is taking place, the customer shall not receive any of this information as such information may be used by the customer in order to “standardize” its behavior or activity or mitigate/destroy evidence needed for investigation

## **9. COMPLIANCE OFFICER**

The AML Compliance Officer, who is also the Director of the company, has several responsibilities which include, but are not limited to, the following:

- Creating, implementing, and maintaining the Company's Policy.
- Conducting training sessions for the Company's staff related to the Policy.
- Developing and managing the risk management approach
- Creating and revising policies, guidelines, and instructions for various departments of the Company within the Program.
- Submitting reports to the FIU as required by the "Reporting to FIU" provision.
- In certain cases, the Compliance Officer has the final approval within the Verification process.
- Communicating with the Company's counterparties regarding AML/CTF matters.

## **10.POSITION OF MLRO**

The responsibilities of Appointing a Money Laundering Reporting Officer (MLRO) include, but not limited to, the following:

- Overseeing the organization's anti-money laundering systems;
- Serving as the focal point for inquiries from regulatory and law enforcement agencies (LEAs);
- Receiving suspicious activity reports (SARs) and making decisions regarding their reporting to authorities;
- Handling regulatory returns/report rendition and monitoring;
- Taking reasonable steps to establish and maintain adequate arrangements for anti-financial crime awareness and training for the organization's staff;
- Obtain and apply relevant regulatory and FATF findings;
- Prepare and send an AML status report to the management committee.

## **11.TRAINING**

The Company provides regular training and workshops for its employees as part of the Policy.

The training covers various topics such as :

- a. the Company's responsibilities under AML-CTF laws;

- b. how to identify suspicious transactions and activities;
- c. how to conduct verifications;
- d. who is considered a Politically Exposed Person etc.

Additionally, priority training is given to employees involved in CDD or EDD measures, and those who handle deposits or withdrawals, such as onboarding specialists, anti-fraud department, payment solution specialists, and support staff who deal with communication on withdrawal/deposit inquiries. The training may also cover other matters relevant to specific departments.

## **12.RECORD-KEEPING**

The Company keeps records of the following data for a period of 5 (five) years from the date of the last transaction or the date when the customer has closed his/her account on any of the Websites:

- a. The information, obtained in the process of the verification and (if applicable) enhanced verification;
- b. The records of transactions (deposits, withdrawals) and their supporting evidence;
- c. The history of communications with customers of the websites.

## **13.REVISIONS OF THIS POLICY**

This Policy is subject to periodical revision. In addition, this Policy may be revised in the following cases:

- a. Changes in legislation;
- b. Changes in the corporate structure of the Company;
- c. Changes in the business profile of the Company;
- d. There are found sufficient deficiencies of this Policy;
- e. In other cases as applicable.

Date of entrance into force:  
27 April 2023

Version as of 19 July 2024