

Know Your Customer Policy

VERSION:

V.1.0

DATE:

07.10.2025

OBJECTIVE:

The aim of this document is to prevent and mitigate specific risks independently of the extent in which they may potentially manifest themselves, defining how these measures and controls are to be applied to particular risk scenarios arising during the performance of Customer Due Diligence.

Version history

Document approver

Version	Date	Approver Contact details
v.1.0.	07.10.2025	MLRO: <i>Edgars Dubins</i>

Table of contents

1. Introduction	2
2. Key Concepts	3
3. Applicability and Regulatory framework	4
4. Customer Acceptance	5
4.1. Customer Due Diligence (CDD)	5
4.2. Timing of CDD Measures	5
4.3. Acceptable documents	7
4.4. Enhanced Due Diligence (EDD)	7
4.5. Ongoing Monitoring	8
5. The Customer Risk Assessment	9
6. Policy Review	10

1. Introduction

INNOVEX B.V.(hereinafter the ‘Company’) commits to the industry goal of keeping crime, and the proceeds of crime out of gambling. Maintaining a safe environment for our customers and our staff is a core pillar of the business. With this respect, the purpose of this document is to obey to what is stipulated under Anti-Money Laundering and Counter-Terrorism Financing Policy of the Company (hereinafter: the “AML and CTF Policy”) on the Know Your Customer Policy.

THE COMPANY’S Know Your Customer Policy provides a description, with non-exhaustive examples, of the type of customers that are likely to pose a higher than average risk of ML/FT and the:

- a. Risk indicators that will lead to a business relationship or an occasional transaction being considered as presenting a Low, Medium or High risk of ML/FT;
- b. Level of CDD measures, including ongoing monitoring to be applied in their relation and under what circumstances the Company will decline to service someone.

THE COMPANY currently does not perform the check of the beneficial owner since its customer base consists of individuals only.

Regarding PEPs, the Company's Senior Management considered them as outside their risk appetite, hence THE COMPANY does not accept any players who may qualify as PEP.

Specifically, the policy is instrumental for the company to ensure it may:

- Carry out risk assessments and identify areas where there may be a heightened vulnerability to ML and TF;
- Prepare, maintain and approve written policies, procedures and controls detailing how the Company manages the risk of ML and TF;
- Review and update the policies, procedures and controls to reflect changes to the risk landscape and the continuously evolving internal approach to AML;
- Provide training and guidance to all employees on how to effectively implement the policies and controls outlined within, and how to monitor the risks and outcomes
- Ensure that adequate resources, funds and systems are in place to support the controls needed to identify, assess and manage AML risks; and
- Monitor the effectiveness and adequacy of the Company's policies and controls, and make improvements where required.

Furthermore, the Policy is in place to ensure a company culture of clear intent, realistic evaluation and actionable processes, in order to carry out the Company goals of combating ML/TF.

2. Key Concepts

Money laundering is the process whereby a criminal / or criminal organization seeks to conceal the true origin of funds or proceeds of crime in order to create the impression that these funds have a legitimate and lawful source.

Money laundering is usually conducted in three stages;

- (1) placement: where the criminal attempts to insert the proceeds of crime into the financial system;
- (2) layering: where the criminal attempts to separate the proceeds of crime from the source and true ownership by a sequence of transactions in order to distort the audit trail and obstruct investigative efforts, followed by;
- (3) integration: the final step where the criminal will introduce the funds with an appearance of being legitimate into the economy, for example; by purchasing real estate, or luxury assets.

Criminal activity can include any kind of conduct that would be a criminal offence in Curacao or any other country in which THE COMPANY operates under its License, including but not limited to terrorism, drug trafficking, activities of criminal organisations, corruption, fraud theft and tax evasion or other tax related offences.

Terrorist financing is where the main focus for concealment is the final destination of the funds, but often also the source in order to dissociate the benefactor of the terrorist organisation, and therefore it may also pass through a process of placement and layering.

3. Applicability and Regulatory framework

The AML/CTF Policy applies to THE COMPANY and will be communicated to all employees of the THE COMPANY, as well as the subsidiaries and sister companies to which THE COMPANY may outsource some of its operations, to ensure they are aware of their responsibilities under AML/TF regulation and the policies set out by the company. For each version update the Know Your Customer Policy will be communicated to staff anew. The policy will also be shared with any third party entering into contract with the Company who has any access to transactional customer data or information which might otherwise present a ML/TF risk.

4. Customer Acceptance

THE COMPANY's Know Your Customer Policy is based on what is required under law and in line with the Company risk appetite and the risk assessment of the business. Certain types of individuals will not be accepted as customers, by either being prevented from registering or blocked from using our site:

- Under 18s;
- PEPs. Politically exposed persons (PEPs) may be subject to pressure and vulnerable to corruption. We do not accept PEPs as customers, and will block any such individual from registering or playing on our site;
- Individuals on EU, UN, UK, FATF or OFAC sanctions lists
- Individuals resident, or located, in countries deemed to be high risk, to measure AML/CTF risk;
- Individuals where we have reason to suspect involvement in ML/TF or other types of criminal activity;
- Self-excluded customers, excluded from our site or any national self-exclusion register available within the licence conditions;
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent;
- Persons who continuously attempt to fund their gambling with deposits from business accounts;
- Customers where an increased risk level in the customer profile for any reason warranted us terminating the customer relationship.

THE COMPANY utilises its internal country risk assessment to determine the risk level of each country, and from which countries it will and will not accept customers. This is based on a combined risk-scoring methodology utilising the FATF, OFAC, UN, EU Sanction list of countries, the Basel AML Index and other reputable sources.

Active customers are monitored, in terms of behaviours and transactions, and should the risk level in the account increase the Company applies enhanced due diligence measures & monitoring. Evaluations are made also if the customer behaviour merits the termination of the business relationship. The expected nature of the customer relationship is that of entertainment. Based on this expectation information is collected, and the profile of a player assessed, in order to identify deviations from the expected customer profile.

4.1. Customer Due Diligence (CDD)

Customer due diligence is carried out as required by our regulatory obligations and in order to sufficiently verify our customers, to be satisfied that the customers are who they say they are, to determine whether customers are acting on behalf of others, and in order to guard the Company against being used for fraud, money laundering or other criminal activity.

THE COMPANY has an obligation to identify the customer when establishing a business relationship and to verify the provided details. As a remote casino operator, the Company must also apply customer due diligence measures in relation to any transaction that amounts to a cumulative €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

4.2. Timing of CDD Measures

THE COMPANY applies CDD measures when carrying out transactions that amount to or exceed €2,000, whether carried within the context of a business relationship or otherwise, and has systems in place to

determine the moment in time when the €2,000 threshold is met. At THE COMPANY the €2,000 threshold, in terms of methodology is calculated:

Taking into account all deposits affected by a customer since the establishment it is calculated on the basis of a rolling period of one hundred and eighty (180) days.

Continuous monitoring is in place to track customer behaviour and where transactions are deemed to be unusual, further investigations are undertaken by the AML Department. These investigations will include, but not be limited to, the following customer behaviours:

- Inactivity period followed by intense activity
- Game type behaviour and amounts played
- Withdrawals amount against Deposits amounts
- Transactional behaviour
- Payment method used
- Any changes to customer profile information
- Communication between Customer Support and the Customer

THE COMPANY may request Source of Funds (SoF) or Source of Wealth (SoW) from the customer for AML or social responsibility reasons should the customer exhibit any of the above behavioural patterns in a negative aspect, if the employee has concerns or is suspicious about the customer, or for any other AML or social responsibility based reason.

i. Source of Funds check:

THE COMPANY interprets SoF as the origin of the money used to fund the customer's transactions with THE COMPANY. THE COMPANY shall establish the bank account or payment method from which the funds were deposited, and the activity involved in generating said funds, such as personal savings, inheritances and gambling winnings.

Where SoF is requested, the employee should verify the documents and should they have any concerns over the source of the funds or the customer's affordability, they will escalate to both the AML and Responsible Gambling teams for further assessment. In such cases the understanding between both departments is that the AML review takes priority.

ii. Source of Wealth check:

THE COMPANY interprets SoW as the total volume of a customer's accumulated wealth, which may include income from employment, business interests and investments. As with SoF checks, the employee will escalate to both the AML and Responsible Gambling teams.

With this respect, the Company must collect sufficient information and where necessary, documentation to establish a customer's source of wealth, as well as the "expected level of activity". Such information is necessary for the THE COMPANY to be able to carry out meaningful ongoing monitoring of transactions since the subject person will only be able to understand and identify the expected behaviour of the customer, including the expected nature of transactions throughout the business relationship, if information obtained is comprehensive.

The above, shall ensure the understanding of the risk posed by each player and to verify whether the SOW justifies the prospective and actual level of account activity.

4.3. Acceptable documents

The following documents are accepted as a means of verification of identity as long as the document contains photographic evidence of the player, is valid and not expired:

- Passport
- National Identification card (photographic)

The following documents are accepted as a means of verification of residential address as long as the document contains the current residential address of the player:

- Official or Bank Correspondence;
- Recent Utility bill (gas, electricity, water, satellite TV, landline phone bill)

THE COMPANY reviews existing records and regularly requests updated documentation from the customers for the purpose of applying CDD measures. Customers are prompted to send updated proof of identity a month before the expiration of the documentation held by THE COMPANY. Proofs of address are updated on a yearly basis notwithstanding the implementation of EDD measures.

4.4. Enhanced Due Diligence (EDD)

Measures of enhanced customer due diligence goes beyond that of the CDD. Enhanced measures are warranted especially in cases identified as high risk

- When a customer or potential customer is a PEP, or a family member or known close associate of a PEP;
- Where the customer is the citizen of a high-risk third country;
- Where a transaction is complex and unusually large, or there is an unusual pattern of transactions;
- Where the customer is situated in a high-risk third country;
- When the risk profile of the customer is high, and any other case which, by its nature; can present a higher risk of money laundering or terrorist financing;

The EDD measures that THE COMPANY applies in case there is a higher risk of money laundering or terrorist financing includes but are not limited to:

- Examining the background of the transaction;
- Increasing the degree and nature of the monitoring of the business relationship, in which the transaction is made, to determine whether that transaction or that relationship appear to be suspicious;

- Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the customer relationship, including greater scrutiny of transactions;
- Seeking additional independent, reliable sources to verify information provided by the customer;
- Taking additional measures to better understand the background, ownership and financial situation of the customer, and other parties to the transaction, i.e.: payslips, savings, inheritance, bank statements, etc.

Enhanced measures may range between utilising information available in open sources to obtaining documentation from the customer to establish and verify SoW/ SoF/ Source of Income (SOI).

4.5. Ongoing Monitoring

THE COMPANY conducts ongoing monitoring of the business relationship, including:

- scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the knowledge of the customer and the customer's risk profile;
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying customer due diligence measures up-to-date.

Customer due diligence measures must also be adopted at other appropriate times to existing customers on a risk-based approach when becoming aware that the circumstances of an existing customer relevant to the risk profile for that customer have changed, such as:

- a change of identity of the customer;
- transactions which are not reasonably consistent with THE COMPANY knowledge of the customer.

Risk assessments of all customers are carried out on an ongoing basis, where the level of customer due diligence will vary depending on the risk profile of the customer.

Suspicious activity will be investigated and reported, and a decision reviewed and made by the MLRO in regards to terminating the customer relationship.

At THE COMPANY we utilise both automated data reporting and manual reviews to carry out risk assessments of all customers on a risk based approach. We have implemented an automated risk scoring solution, which evaluates all player activity based on multiple risk flags which could indicate ML/TF activity, and assigns a risk score to the customer account where customers with a higher score are subject to manual AML reviews. In addition to this, we also have specific alerts to flag activity that warrants an AML review.

i. Risk scoring and automated alerts

The THE COMPANY AML risk score is based on known indicators of potential ML, enabling the identification and scrutiny of unusual patterns of transactions. The automated score is regularly reviewed

and improved to enhance accuracy. In addition to the score, alerts are in place to highlight activity that warrants increased scrutiny.

ii. Manual Reviews

Our customer-facing staff, and employees that review customer accounts and activity in their daily tasks, are trained to recognise activity that should warrant further investigation, and will in these cases submit an internal suspicious activity report to the MLRO for further review.

THE COMPANY implements further manual controls based on the risk level of the account. Trained staff will review the account and activity therein to evaluate if there is reasonable grounds for suspicion or if the activity can be explained with further investigation, documentation and/or other means.

Higher risk customers will also be added to a monitoring list, in order for continuous manual checks over a period of time, depending on the particular case. If the risk profile of a customer increases beyond the company's risk appetite, and suspicious activity is detected, a report will be made and the customer relationship terminated.

5. The Customer Risk Assessment

The Customer Risk Assessment (CRA) that THE COMPANY has implemented, categorises our customer base in the following levels of AML risk: Low, Medium & High.

This AML risk score is comprised of various risk criteria divided into two categories:

- Behavioural
- Structural

The following are the criteria that form part of the **Behavioural category**:

- Expenditure Trend (Average amount of real bets divided by the average amount of deposits)
- Betting frequency (Number of real bets divided by number of deposits)
- Rentability (Deposit amount - GGR / deposit amount)

*Behavioural risk Level: As the sum of the 3 above scorings

The following are the criteria that form part of the **Structural category**:

- Payment Element Score which is calculated by the number of used payment methods;
- Prepaid ratio which is the ratio of prepaid deposits out of the total number of deposits made (prepaid is when method and card category are prepaid);
- Card Bin Score which is calculated by the risk rating given to the jurisdiction the player is coming from, makes transactions to/from the said high risk jurisdiction, sanctioned/monitored jurisdiction.
- Product Score: whether the player only played Slots or other games.

6. Policy Review

The persons responsible for designing, monitoring and updating these internal controls are the MLRO and the members of the AML Department.

The approver of The Policy is the MLRO. In addition to this the Policy will be reviewed and approved by the board on an annual basis at minimum, or in case significant changes are done at a level which warrants a Board approval.

The company will perform an annual assessment on the risks inherent to the products when reviewing the policy. This assessment shall help to update the AML/CTF policy and the related procedures.

The MLRO and the AML Department will review the AML/CTF Policy on an annual basis at minimum, or whenever circumstances change to warrant a review and update of the document as set out by the following criteria:

- A. annually, no later than 12 months from the date upon which the Policy was last reviewed;
- B. following any recommendations resulting from an audit or risk assessment that the Policy requires amendment;
- C. upon the change of any relevant law or regulation which applies to the Policy;
- D. upon the finding by any regulator that an amendment to the Policy is required;
- E. upon the acceptance of customers from a jurisdiction / territory where company did not previously accept customers;
- F. upon acquiring a new product / vertical;
- G. whenever significant changes occur in the business, that will have a direct or indirect impact on the area this document concerns.

Any amendment of the Policy shall, as soon as is reasonably practicable, be distributed or informed to all persons within the scope of the Policy for information of the amendment. Any change in Policy giving rise to a Procedure review shall be identified and such changes shall be implemented to the relevant Procedure. The Policy approver is responsible for making sure that the Policy is reviewed and updated on a regular basis as set out in this section.