

Horizonix Corp N.V.
Know Your Customer (KYC) Policy
version 1.0

1. Purpose and Policy Statement

This Know Your Customer (KYC) Policy (“Policy”) is adopted and implemented by Horizonix Corp N.V., a company duly incorporated and existing under the laws of Curaçao, having company registration number 166811, with its registered office at Hanchi Snoa 19, Trias Building, Willemstad, Curaçao (the “Company”).

This Policy sets out the principles, rules and procedures applied by the Company to identify, verify and monitor its customers in order to prevent the misuse of its gaming services for money laundering, terrorist financing or other unlawful purposes.

The Company operates under a valid gaming licence issued in Curaçao and is subject to the supervision of the Curaçao Gaming Authority. The Company is committed to full compliance with applicable Curaçao legislation, regulatory requirements, and international standards in the field of AML/CTF and responsible gaming.

This Policy forms an integral part of the Company’s compliance framework and shall be applied together with the AML-CTF Policy, Responsible Gambling Policy, internal procedures for Customer Support, and other compliance documents.

2. Scope of Application

This Policy applies to all customers (players) of the Company, regardless of the registration method used, the payment method selected, or the transaction volume. It also applies to all employees, contractors and third parties involved in customer onboarding, verification, monitoring, payments, withdrawals or customer interaction.

The Policy covers standard registration flows as well as simplified or accelerated registration models, including one-click registration.

3. Regulatory Framework

This Policy is established in accordance with, inter alia:

- the National Ordinance on Identification when Rendering Services (NOIS, PB 2017, no. 92);
- the National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017, no. 99);
- the National Ordinance on Games of Chance (PB 2024, no. 157);
- the Regulations for the Combating of Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction (January 2025);
- binding instructions and guidance issued by the Curaçao Gaming Authority.

KYC obligations are applied as an operational extension of the Company’s AML/CTF framework.

The Company performs customer identification and verification in accordance with the applicable laws and regulations of Curaçao, including AML/CTF legislation, sanctions legislation, the National Ordinance on Games of Chance, and the AML-CTF regulations and guidance issued by the Curaçao Gaming Authority.



The Policy also reflects relevant FATF Recommendations and internationally recognised AML/CTF standards to the extent applicable.

4. Risk-Based Approach

The Company applies a risk-based approach to KYC. The scope, timing and depth of customer due diligence measures depend on the level of risk associated with a particular customer.

Customer risk is assessed by reference to factors such as geographic location, transaction behaviour, payment methods, registration channel, potential sanctions or PEP exposure, and any indicators of attempted circumvention of controls. Based on this assessment, simplified, standard or enhanced due diligence measures are applied.

5. Prohibition of Anonymous and Fictitious Accounts

The Company does not permit anonymous accounts or accounts registered under false or fictitious identities. Even where simplified or one-click registration is used, the Company ensures that sufficient identifying information is collected to uniquely identify the customer and to enable subsequent verification.

6. Customer Information Collected at Registration

At the time of registration, the Company collects basic identifying information necessary to establish a customer account. This includes, at a minimum:

- the customer's full name (First Name and Last Name),
- date of birth and
- permanent residential address, as well as contact details and account credentials.

The information collected at the registration stage is intended to establish a customer account and does not constitute full customer due diligence within the meaning of this Policy and AML/CTF regulations.

The customer must confirm acceptance of the Terms and Conditions and declare that they are acting on their own behalf.

7. One-Click Registration and Initial Controls

Where the Company offers one-click or accelerated registration, such model is implemented strictly within the limits permitted by regulation and the Company's risk appetite.

Before or at the moment of account creation, customers are subject to automated screening, including geolocation controls, age-eligibility validation* and checks against restricted or sanctioned jurisdictions. Access from prohibited jurisdictions is blocked, and accounts are not created where such access is detected.

Where one-click registration is used, it serves only to streamline onboarding. Geolocation controls, country, age-eligibility validation, and checks against restricted or sanctioned jurisdictions remain mandatory and are applied as part of the one-click registration flow, with any non-eligible users being denied access, as stated above.



One-click registration does not exempt customers from full KYC requirements, which are applied at later stages in accordance with this Policy and our AML/CTF Policy.

* The Company's system prohibits the registration of underage customers. To successfully complete the registration process, customers must be at least 18 years of age or meet the legal age requirement in their jurisdiction. The provided date of birth will be verified against identification documents during the customer due diligence process.

8. Restricted and Sanctioned Jurisdictions

The Company maintains and regularly updates a list of restricted and prohibited jurisdictions. This list includes jurisdictions subject to international sanctions, jurisdictions classified by FATF as high-risk or under increased monitoring, and jurisdictions restricted due to regulatory or licensing considerations.

Customers located in, or attempting to access the services from, restricted jurisdictions are not permitted to register, deposit, withdraw or participate in games. Attempts to circumvent geo-blocking measures are treated as high-risk events and may result in account suspension, enhanced due diligence or termination of the business relationship.

9. Circumstances Triggering Customer Identification and Verification

The Company is legally required to identify and verify customers not only at onboarding, but also at specific stages of the business relationship and upon the occurrence of defined triggering events.

9.1. Establishment of the Business Relationship

For the purposes of this Policy, a business relationship is deemed to be established when a customer account is created and access to gaming services is granted, including via accelerated or one-click registration, subject to regulatory limits on deferred verification.

Upon establishing a business relationship, the Company collects sufficient information to identify the customer and prevent anonymous use of the website. Where simplified or one-click registration is applied, this initial stage is combined with real-time screening controls and deferred verification, subject to regulatory limits.

9.2. First Withdrawal Attempt

The Company completes customer identification and verification no later than the first attempt by a customer to withdraw funds, where full verification has not already been completed. This applies to all registration flows, including one-click or accelerated registration. No withdrawal is processed until the required KYC/CDD checks are successfully completed and approved by the Company.

9.3. Financial Thresholds

Full customer due diligence is mandatory once the amount of a single transaction, or a series of linked transactions, reaches or exceeds approximately ANG 4,000 (or its equivalent).



This threshold applies to both deposit and withdrawal transactions and is calculated on a cumulative basis from the start of the business relationship. The Company's systems monitor transaction volumes to ensure timely identification and verification.

9.4. Occasional Transactions

Customer identification and verification is also required where a customer conducts an occasional transaction, outside of an established business relationship, in the amount of ANG 4,000 (or its equivalent) or more.

9.5. Suspicion of Money Laundering or Terrorist Financing

The Company immediately performs identification and verification, including enhanced due diligence where appropriate, whenever there is a suspicion of money laundering, terrorist financing or other criminal activity.

Such suspicion may arise from unusual transaction behaviour, inconsistencies in customer information, attempts to avoid verification, or red flags identified by Customer Support, compliance systems or third-party providers.

9.6. Doubts About Customer Data

If the Company has doubts regarding the accuracy, completeness or authenticity of customer data or documents previously obtained, re-verification is initiated without delay. The Company does not rely on information whose reliability is questionable.

9.7. Changes in Risk Profile

Customers are re-assessed and, where necessary, re-verified when there is a material change in their risk profile, including significant changes in transaction behaviour, payment methods, geographic indicators or PEP/sanctions exposure.

9.8. One-Click Registration Context

Where customers register via one-click registration, KYC obligations are deferred only to the extent permitted by regulation. In any case, full identification and verification is completed upon the first withdrawal attempt, upon reaching the financial threshold, or earlier if risk indicators arise.

10. Scope of Customer Due Diligence

As part of KYC, the Company collects and verifies, at a minimum:

- the customer's full name (First Name and Last Name),
- date of birth and
- permanent residential address, as well as contact details and account credentials.

Additionally, geolocation controls and additional monitoring of the customers use of VPN tools are also constantly carried out.

Depending on the risk level, additional data such as:

- place of birth,



- nationality,
- identification number and source of funds may be required.

In all cases, CDD procedures must be fully performed by the Company in accordance with this Policy and our AML/CTF Policy, not only at onboarding, but also at specific stages throughout the business relationship and upon the occurrence of defined triggering events (Such specified events are specified in section 9 of this Policy).

Identity is verified using valid government-issued documents, and address verification is performed using reliable documents not older than three (3) months. Electronic verification tools may be used where they provide equivalent reliability. For this purpose, the Company may engage reputable third-party service providers (KYC providers) to assist in the customer identification and verification process. Such providers may use electronic means, automated systems and technological solutions to verify the authenticity of identification documents, perform biometric and liveness checks, and verify the customer's identity.

The use of third-party KYC providers does not relieve the Company of its regulatory obligations, and the Company remains fully responsible for compliance with applicable AML/CTF and regulatory requirements.

Verification of Identity

The Company maintains internal procedures to confirm the identity of its customers and to ensure that the personal information associated with a customer account is accurate, current and attributable to the individual using the services.

Identity verification is conducted as part of the Company's customer due diligence framework and is based on information obtained from reliable and independent sources. The objective of this process is to achieve an appropriate level of certainty regarding the customer's identity, taking into account the nature of the relationship and the associated risk.

As part of its verification procedures, the Company requests official identification documents issued by competent governmental authorities and containing a photograph of the customer. The Company assesses whether the documents provided are complete, legible and suitable for verification purposes before accepting them.

Where confirmation of a customer's residential address is required and is not evident from the identification document, the Company obtains separate evidence to establish the address. Such evidence may consist of financial documents issued by regulated institutions, utility-related documentation, official correspondence or contractual documents relating to residential premises. The Company applies internal standards regarding the recency and reliability of such documents.

The Company uses secure communication and authentication methods to validate customer contact details and to ensure that the information provided can be reliably linked to the customer account. These methods may include verification links, one-time authentication codes or direct confirmation through registered communication channels.

To support the verification process, the Company may corroborate customer information using additional data sources that are appropriate to the customer's risk profile. This may include the use of publicly accessible information, commercial databases or adverse media sources, where such checks are lawful and proportionate.



Where deemed appropriate, the Company applies technological solutions as part of its verification framework. Such solutions may include biometric comparison, liveness detection or other technical measures designed to confirm that the person interacting with the account corresponds to the identity presented.

The Company may also assess the internal consistency of customer information by comparing customer-provided data with technical and transactional indicators available within its systems, including device-related data, geolocation signals, IP information or payment-related data, where this assists in identity validation or risk management.

To enhance the efficiency and reliability of its verification procedures, the Company may engage specialised third-party service providers to support identity verification activities. These providers may use automated systems and electronic verification methods in line with the Company's requirements. The Company remains responsible for the outcome of the verification process and for compliance with all applicable legal and regulatory obligations.

Where the outcome of verification does not provide sufficient confidence, or where discrepancies or risk indicators are identified, the Company applies additional verification steps proportionate to the circumstances. Such steps are determined by the Company based on its internal risk assessment.

In cases involving documentation issued outside commonly used jurisdictions or in unfamiliar formats, the Company applies increased scrutiny to ensure that such documentation is appropriately validated before the customer relationship is maintained.

Restriction on Deposits , Betting and Withdrawals Pending Completion of KYC and CDD

The Company applies a staged, risk-based approach to access to deposits, wagering and withdrawals. Where a customer registers using simplified or one-click registration, the account may be created to streamline onboarding; however, access to financial and gaming functionalities is enabled only to the extent permitted by regulation and the Company's risk appetite.

At a minimum, prior to enabling any deposit or wagering functionality, the Company performs mandatory automated controls, including geolocation and jurisdictional restriction checks, sanctions screening and age-eligibility validation. Access from prohibited or sanctioned jurisdictions is blocked and accounts are restricted accordingly.

Full identification and verification (including documentary and/or electronic verification and any enhanced checks required by the customer's risk profile) is completed before (i) any withdrawal is processed, and (ii) once the customer reaches the applicable financial thresholds or other defined triggering events under Section 9 (including Section 9.3), or earlier where risk indicators arise.

In cases where KYC or CDD is pending, incomplete or under review, the Company applies technical and operational measures to restrict deposits, betting and gameplay. Such restrictions remain in place until the verification process is concluded to the Company's satisfaction or the customer relationship is otherwise terminated.

11. Sanctions and PEP Screening



All customers are screened against applicable sanctions lists and assessed for PEP status at onboarding and on an ongoing basis. Customers subject to sanctions are not accepted, and any funds involved are handled in accordance with applicable law.

Decisions to approve, restrict, suspend or terminate a customer relationship on KYC grounds are taken by or under the authority of the Compliance function. Customer Support may not override KYC decisions.

Customers identified as PEPs are subject to enhanced due diligence, including senior management approval and enhanced monitoring.

12. Ongoing Monitoring

The Company conducts ongoing monitoring of customer activity to ensure consistency with the customer's profile and declared information. Monitoring covers transactions, payment behaviour, gameplay patterns and compliance with responsible gaming requirements.

Customer data is kept up to date and refreshed as required.

13. Failure to Complete KYC

If a customer fails to provide the required information or documents within the prescribed timeframe, the Company may restrict or suspend access to the account until verification is completed. Continued non-compliance may result in termination of the business relationship, subject to legal and regulatory obligations.

14. Record Keeping and Data Protection

All KYC records are retained for the period required by Curaçao law and stored securely. KYC records and verification data shall be made available without delay to the Curaçao Gaming Authority, the Financial Intelligence Unit Curaçao or other competent authorities upon lawful request. Personal data is processed in accordance with applicable data protection requirements.

15. Review

Updates are made to reflect changes in legislation, regulatory guidance or the Company's risk assessment.

Signed This of January 5, 2026



Director: Ecorpp Management N.V.