

HORIZONIX CORP N.V.

AML/CTF Policy

Version 4.0

KEY INFORMATION	3
1. Policy Statement	4
2. Purpose	5
3. Audience	6
4. Definitions	7
5. Policy Implementation	8
5.1. Information Entered on Registration	8
5.2. Terms Acceptance	9
5.3. Underage Customers	9
5.4. Business Risk Assessment (BRA)	9
5.5. Customer Risk Assessment (CRA)	9
5.6. Customer Acceptance Policy (CAP)	11
5.7. Customer Due Diligence (CDD)	12
☐ CDD Measures:	12
☐ Enhanced Due Diligence (EDD):	13
5.8. Ongoing Monitoring	13
5.9. Reliance on Third Parties for CDD	14
5.10. Reporting of Suspicious Transactions	14
5.11. Anti-Money Laundering Compliance Program	15
6. Compliance and Consequences of Non-Compliance	17
7. Related Information	18
8. Contact Information	19
9. Policy History	20
10. Policy URL	21
Appendix 1	22

Key Information

Approving Official(s):	Ecorpp Management N.V., Director Horizonix Corp N.V.
Responsible Office:	Compliance Department, Horizonix Corp N.V.
Effective Date:	January 09, 2026
Next Review Date:	January 09, 2027 (initial review within one year, subsequent reviews every three years)

1. Policy Statement

Horizonix Corp N.V. ("the Company"), a duly incorporated under the laws of Curaçao (Registration No. 166811; Registered Office: Hanchi Snoa 19, TRIAS Building, Curaçao; holding a valid license issued by the Curaçao Gaming Authority), is steadfastly committed to ensuring that its services, products, and infrastructure are not exploited for money laundering (ML), terrorist financing (TF), or the financing of proliferation of weapons of mass destruction (FP). The Company strictly complies with the legislative framework of Curaçao, including the National Ordinance on Identification when Rendering Services (NOIS, N.G. 2017, no. 92), the National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99), the National Ordinance on Games of Chance (NOGC, N.G. 2024, no. 124), the National Ordinance Penalization of Money Laundering (NOPML), the Sanctions National Ordinance (N.G. 2014, no. 55), and the Kingdom Sanction Act (N.G. 2016, no. 54). Furthermore, the Company adheres to the FATF Recommendations and relevant EU Directives, including Directives 2015/849, 2018/843, and 2018/1673. This policy extends to all employees, contractors, third-party representatives, and business partners engaged in the Company's operations.

2. Purpose

This AML/CTF Policy is designed to ensure adherence to Curaçao's legal framework and international standards, including the "Regulations for Combating Money Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction" (effective January 9, 2025), the FATF Recommendations, and relevant EU Directives. The objectives of this policy are to:

- Safeguard the Company's reputation and operational integrity against risks associated with financial crimes.
- Adopt a risk-based methodology to identify, evaluate, and mitigate risks related to ML, TF, and FP.
- Implement customer due diligence (CDD), transaction monitoring and suspicious activity reporting mechanisms applicable to the Company's B2C online gaming operations.
- Promote a culture of compliance through regular employee training, thorough background checks, and effective internal control measures.
- Prevent predicate offenses to ML/TF, such as fraud, as outlined in EU Directive 2018/1673 and other applicable legislative frameworks.

3. Audience

This policy encompasses:

- All employees, officers, and directors of Horizonix Corp N.V.
- Third-party service providers, agents, and subcontractors engaged in the Company's operational activities.
- B2C customers (players) using the Company's online gaming services.

4. Definitions

- **Casino:** Denotes the online gaming operations conducted by Horizonix Corp N.V.
- **Financial Transactions:** Encompasses deposits, withdrawals, wire transfers, and currency exchanges, excluding gambling-related transactions such as wagers or winnings.
- **FIU:** Refers to the Financial Intelligence Unit Curaçao, tasked with receiving Suspicious Activity Reports (SARs).
- **Politically Exposed Persons (PEPs):** Individuals holding prominent public positions, their immediate family members, or close associates, as defined under EU Directive 2015/849 and other applicable legislative frameworks.
- **Suspicious Transaction:** A transaction exhibiting objective or subjective indicators as stipulated under NORUT, including transactions of NAf. 4,000 or greater, or those suspected of involvement in ML/TF activities.
- **Ultimate Beneficial Owner (UBO):** The natural person(s) who ultimately own or control a customer or entity, holding at least 25% of shares or voting rights, or exercising ultimate control, as per EU Directive 2018/843 and other relevant legislation.
- **Source of Funds (SoF):** The origin of funds used in a specific transaction, such as salary or gambling winnings.
- **Source of Wealth (SoW):** The origin of a customer's total accumulated wealth, derived from sources such as employment or investments.
- **Predicate Offense:** Criminal activities that generate proceeds subject to laundering, as specified in EU Directive 2018/1673, including offenses such as fraud or corruption.

5. Policy Implementation

The Company implements a risk-based approach to AML/CTF compliance, as required by the Curaçao Gaming Authority (CGA, previously known as the Curaçao Gaming Control Board) and the FATF Recommendations. The subsequent sections delineate the framework for its execution.

This Policy constitutes the Company's primary Anti-Money Laundering (AML) policy and is applied in conjunction with the Company's Know Your Customer (KYC) Policy, which serves as a supplement to and continuation of this Policy. The KYC Policy sets out the customer identification and verification procedures implemented in furtherance of the requirements established under this AML Policy.

5.1. Information Entered on Registration

During the registration process, the Company collects a limited set of information necessary to create a customer account and to perform initial screening. The information collected at this stage does not constitute customer due diligence and is supplemented by additional identification and verification measures at later stages in accordance with the Company's KYC Policy.

At the registration stage, the Company collects the following information:

- Full name (first name and last name).
- Date of birth.
- Permanent residential address.
- Contact details, including an email address and/or, where applicable, a mobile phone number.
- Account credentials (username and password).

Geolocation controls, country, age-eligibility validation, and checks against restricted or sanctioned jurisdictions remain mandatory.

Identification documents, proof of address and other verification materials are not collected at the registration stage. Such information and documentation are requested only when customer due diligence is triggered in accordance with the Company's know Your Customer (KYC) Policy, including, inter alia, upon the first withdrawal attempt, upon reaching the applicable monetary threshold, and/or where required based on the customer's risk profile.

Where one-click or accelerated registration is used, it serves solely to streamline the onboarding process and does not remove or replace the Company's customer due diligence obligations. As part of the one-click registration flow, the Company applies mandatory preliminary controls, including geolocation checks, country-of-residence screening, age-eligibility validation, and automated checks against restricted and sanctioned jurisdictions. Customers who do not meet eligibility criteria or who are identified as accessing the services from prohibited jurisdictions are denied access to the website at the registration stage.

5.2. Terms Acceptance

During the registration process, the customer must also confirm acceptance of the website's.

5.3. Underage Customers

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.

5.4. Business Risk Assessment (BRA)

Objective: Identify and mitigate ML/TF/FP risks inherent to the Company's operations.

Procedure:

- The Compliance Department conducts an annual BRA, updated upon significant changes (e.g., new products, markets, or regulations).
- The BRA evaluates:
 - **Customer Risk:** Risks from high spenders, PEPs, or customers with irregular income.
 - **Geographical Risk:** Exposure to high-risk jurisdictions (e.g., FATF High-Risk Jurisdictions <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>, EU Directive 2018/843 Annex II countries).
 - **Product/Service Risk:** Risks from products allowing anonymity (e.g., prepaid cards, cryptocurrencies) or high-stake games (e.g., roulette).
 - **Distribution Channel Risk:** Risks from non-face-to-face interactions or third-party intermediaries.
- Sources consulted include FATF lists, CFATF statements, Transparency International's Corruption Perceptions Index, EU sanctions lists, and the U.S. INCSR.
- The BRA is documented, approved by the Board of Directors, and submitted to the CGA upon request.
- Outcomes inform the Company's risk appetite and AML/CTF controls, ensuring alignment with FATF Recommendation 1 (risk-based approach).

5.5. Customer Risk Assessment (CRA)

Objective: Assess ML/TF/FP risks posed by players.

- Conducted at onboarding and updated during the business relationship.
- Factors assessed (per FATF Recommendation 10 and EU Directive 2015/849):
 - **Individual Status:** PEP status, sanctions/blacklist presence, adverse media.
 - **Geographical Location:** Residence in high-risk countries (e.g., FATF black/grey lists, Appendix 1).

• **Gambling/Transactional Behavior:** Large deposits with minimal play, smurfing, or disproportionate spending.

• **Payment Methods:** Use of high-risk methods (e.g., vouchers, cryptocurrencies, prepaid cards). Payment Methods are also divided into:

Payment Method	Risk Rating
Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks	Low
EEA licensed e-wallets (Skrill, Neteller, paysafecard)	Medium
Vouchers, cryptocurrencies, prepaid cards	High

• **Fraud Indicators:** VPN usage, multi-accounting, or synthetic identities.

- Risk ratings (low, medium, high) determine CDD levels:

• **Low (0–20):** Basic CDD, minimal monitoring.

• **Medium (21–40):** Standard CDD, additional personal details, SoF checks.

• **High (41+):** Enhanced Due Diligence (EDD), SoF/SoW documentation, enhanced monitoring.

- Risk scores are calculated based on weighted indicators (e.g., PEP status: 100 points, high-risk country: 30 points). More details in the table below:

Indicator	Description	Score
individual status		
<i>PEP</i>	A customer considered to be PEP	100
<i>Adverse media</i>	A customer was mentioned in negative news or information the company discovered from various sources	50
<i>Sanctions/blacklist</i>	A customer is under international sanctions/blacklists	100
geographical location		
<i>Not at home</i>	A customer whose IP location is different from their registered address	20
<i>High-risk country resident</i>	A customer resides in a High-risk country	30
gambling behavior		
<i>Large sums no play</i>	A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds	50
<i>Large sums big losses</i>	A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence (EUR 5000 per week)	50
<i>Low odds betting</i>	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favorites) bets	25

<i>Big changes in money</i>	Dramatic changes in terms of volume and size of player deposits or staking activity	20
<i>Several gaming accounts</i>	A customer is trying to register several gaming accounts	30
transactional behavior		
<i>Smurfing</i>	A customer making multiple deposits or withdrawals of small amounts without no objective reasons	30
<i>Spending above wages</i>	A customer's spend is outside of their affordability	20
<i>No withdrawals</i>	Player has never requested a withdrawal	-20
<i>Withdrawal without playing</i>	Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling	30
payment methods the player is using		
<i>Card switching</i>	A customer opening an account and registering several different cards and making transfers between them	20
<i>High risk payment methods</i>	A customer uses high-risk payment methods	30
fraud red flags a customer triggered		
<i>VPN</i>	Customer used a VPN	30

5.6. Customer Acceptance Policy (CAP)

Objective: Define criteria for accepting B2C customers (players).

Procedure:

- The CAP specifies:

- **High-Risk Customers:** PEPs, sanctioned entities, residents of FATF black/grey-listed countries (Appendix 1), or those with adverse media.
- **Risk Indicators:** Multiple accounts, high-risk payment methods, or fraud red flags.
- **CDD Measures:** Simplified (SDD), standard, or enhanced (EDD) based on risk level.
- **Grounds for Rejection:**

√ Underage individuals (< 18).

√ Sanctioned entities or PEPs (automatic rejection per EU Directive 2015/849), the Consolidated United Nations Security Council Sanctions List 12, the Sanction Decree "Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s." (N.G. 2015, no. 29), the Ministerial Regulation "Libya" (N.G. 2015, 28), the Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27);, the Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30), and the Ministerial Regulation "Yemen" (N.G. 2015, 65).

✓ Incomplete CDD within 14 days.

✓ Fraudulent behavior, bonus abuse, or terms breaches.

✓ Existing customers who have an existing exclusion on the site.

✓ Individuals with fraud red flags.

✓ Entities directly or indirectly owned by any PEP.

- Players are declined if they fail to provide CDD documentation or are listed on sanctions lists.
- Geo-blocking restricts access from prohibited jurisdictions (Appendix 1).

5.7. Customer Due Diligence (CDD)

Objective: The Company shall authenticate customer identities and implement measures to mitigate risks associated with money laundering (ML), terrorist financing (TF), and the financing of proliferation of weapons of mass destruction (FP), in accordance with FATF Recommendation 10 and EU Directive 2015/849.

- When CDD is Required:

- Financial transactions $\geq$ Naf. 4,000 or EUR 2,000 (single or linked), per EU Directive 2018/843.
- At the first attempt by a customer to withdraw funds, where full identification and verification have not yet been completed;
- Suspected ML/TF activity or predicate offenses (e.g., fraud, per EU Directive 2018/1673), regardless of the transaction amount;
- Where a material change in the customer's risk profile is identified through ongoing monitoring.
- Doubts about previously obtained identification data.
- Other cases where the Company determines that Customer Due Diligence (CDD) is necessary.

Until the required CDD measures have been completed to the Company's satisfaction, the customer account remains subject to appropriate restrictions in accordance with the Company's Know Your Customer (KYC) Policy and internal procedures, or the business relationship is otherwise terminated where required by law.

□ CDD Measures:

- **Identification:** the minimum identification data consists of the customer's full name, date of birth and permanent residential address, in line with the Company's Know Your Customer (KYC) Policy. Additional identification data is collected only where required based on the customer's risk profile or applicable regulatory triggers.
- **Verification:** Use unexpired government-issued photo ID (e.g., passport, driver's license). Address verification is performed using reliable supporting documentation in accordance with the Company's Know Your Customer (KYC) Policy and/or internal

risk-based standards.

- **UBO Identification:** Ensure players act on their own behalf via terms and conditions. For syndicate-funded accounts, identify and verify UBOs.
- **Purpose of Relationship:** Establish expected activity levels using customer declarations or statistical data.
- **Sanctions/PEP Screening:** Screen against UN, EU, and Curaçao sanctions lists and PEP databases (e.g., knowyourcountry.com).

□ Enhanced Due Diligence (EDD):

Enhanced due diligence measures are applied to customers assessed as high-risk in accordance with the Company's risk assessment framework and Know Your Customer (KYC) Policy. High-risk factors may include, inter alia,

- Politically exposed person (PEP) status,
- Indicators of heightened money laundering or terrorist financing risk, or
- Other circumstances identified through ongoing monitoring.

EDD measures may include:

- Verification of the source of funds and, where appropriate, the source of wealth.
- Enhanced scrutiny of transactions and customer behaviour.
- Where required by the nature of the risk, the continuation of the business relationship may be subject to approval by senior management.
- **Simplified Due Diligence (SDD):** Simplified due diligence may be applied to customers assessed as low-risk, in accordance with the Company's risk-based approach and applicable regulatory requirements. In such cases, the scope of identification and verification measures is limited to the minimum required under the Company's Know Your Customer (KYC) Policy.
- **Freezing of Funds:** If a customer is sanctioned or ML/TF is suspected, funds are frozen, and a SAR is filed with the FIU within 7 days. Accounts are blocked if CDD is incomplete after 14 days, with funds returned to the original source unless ML/TF is suspected.
- **Ongoing Monitoring:**
 - Refresh ID upon document expiry or profile changes.
 - Monitor transactions for inconsistencies (e.g., large deposits, smurfing).

5.8. Ongoing Monitoring

Objective: Ensure customer activity aligns with risk profiles and detect suspicious behavior.

- **Identity Monitoring:** Refresh identification upon key events (e.g., payment method changes) or document expiry.

- **Transaction Monitoring:** Scrutinize transactions for inconsistencies (e.g., large deposits with minimal play, card switching). Investigate SoF for deviations.
- **Behavioral Monitoring:** Identify patterns indicative of ML/TF (e.g., low-odds betting, smurfing) or problem gambling.
- **Risk Profile Updates:** Reassess risk ratings if significant changes occur (e.g., new PEP status).
- **High-Risk Customers:** Conduct enhanced monitoring, including frequent SoF/SoW checks.

5.9. Reliance on Third Parties for CDD

Objective: Ensure compliance when delegating CDD tasks, per FATF Recommendation 17 and EU Directive 2015/849.

Procedure:

- The Company may rely on third parties (e.g., payment processors) for identification, verification, and purpose of relationship data, provided:
 - The third party is regulated and complies with Curaçao or equivalent AML/CTF standards.
 - An agreement ensures immediate access to CDD data.
 - The arrangement is tested periodically for effectiveness.
- The Company remains responsible for CRA, PEP screening, and ongoing monitoring.
- Outsourcing to agents requires the Company's AML/CTF policies to be applied, with regular compliance audits.

5.10. Reporting of Suspicious Transactions

Objective: The Company shall identify and report transactions suggestive of money laundering (ML), terrorist financing (TF), or the financing of proliferation of weapons of mass destruction (FP), in compliance with FATF Recommendation 20 and EU Directive 2015/849.

Procedure:

- **Recognition:** Employees are trained to identify suspicious transactions, including:
 - Transactions $\geq$ Naf. 4,000 or EUR 2,000 (cash, cashless, chips, or withdrawals).
 - Transactions reported to authorities for ML/TF or predicate offenses.
 - Transactions involving sanctioned entities or PEPs.
 - Red flags (e.g., large deposits with minimal play, frequent small transactions, third-party withdrawals).
- **Internal Reporting:** Employees submit Internal Suspicious Activity Reports (SARs) to the Compliance Officer, including customer details, employee statements, and supporting documents.

- **External Reporting:** The Compliance Officer submits SARs to the FIU via the goAML portal within 7 days of detection, in English, with all relevant documentation.
- **Account Blocking:** If ML/TF is suspected, accounts may be blocked to prevent tipping off (per EU Directive 2015/849, Article 41). Funds are frozen if sanctions apply.
- **Tipping Off:** Employees are prohibited from informing customers about SARs or investigations to avoid prejudicing inquiries.
- **Record Keeping:** All transaction records, SARs, and CDD data are retained for ≥ 5 years post-relationship or transaction, per FATF Recommendation 11.

5.11. Anti-Money Laundering Compliance Program

Objective: Establish a robust framework to mitigate ML/TF/FP risks.

Procedure:

- **Internal Policies and Controls:**
 - Policies express senior management's commitment to AML/CTF compliance.
 - Procedures detail CDD, KYB, reporting, and monitoring processes.
 - Internal controls detect deviations (e.g., automated transaction monitoring).
- **Compliance Officer:**
 - A senior officer, independent from gaming operations, oversees the AML program.
 - Responsibilities include risk analysis, policy development, training, SAR submission, and FIU liaison.
 - The officer has authority to issue instructions and conduct random checks.
- **Employee Training:**
 - New employees receive AML/CTF training, including recognition of predicate offenses (EU Directive 2018/1673).
 - Frontline staff (e.g., cashiers) are trained on ML techniques, red flags, and reporting.
 - Annual refresher training covers new trends and regulatory updates.
 - Training records include content, attendees, dates, and test results.
- **Employee Background Checks:**
 - Pre-employment checks include ID, CV, and integrity assessments.
 - Annual screenings ensure compliance, with surprise checks for high-risk roles.
- **Independent Audit:**
 - Conducted annually by a qualified external auditor (≥ 2 years AML experience, CAMS certification).

- Tests include policy evaluation, customer file reviews, transaction testing, and training adequacy.
- Findings are reported to senior management with corrective action deadlines.

- Account Blocking Procedure:

- Accounts are blocked if CDD is incomplete after 14 days, ML/TF is suspected, or sanctions apply.
- Funds are returned to the original source unless ML/TF suspicions or sanctions require freezing and FIU reporting.

6. Compliance and Consequences of Non-Compliance

Compliance:

- All employees and third parties must adhere to this policy.
- The Compliance Officer monitors implementation and reports to senior management.

Consequences of Non-Compliance:

- **Employees:** Disciplinary actions, up to termination, for policy violations.
- **Third Parties:** Termination of contracts for non-compliance.
- **Legal Risks:** Administrative fines or criminal sanctions under NOIS, NORUT, NOPML, or Sanctions National Ordinance.
- **Business Risks:** Reputational damage or license revocation by the CGA.

7. Related Information

- **Regulations:** NOIS (N.G. 2017, no. 92), NORUT (N.G. 2017, no. 99), NOGC (N.G. 2024, no. 124), NOPML, Sanctions National Ordinance (N.G. 2014, no. 55), Kingdom Sanction Act (N.G. 2016, no. 54).
- **International Standards:** FATF Recommendations, EU Directives 2015/849, 2018/843, 2018/1673.
- **Guidelines:** Curaçao CGA Regulations for combating ML/TF/FP (January 2025).
- **Resources:** UN Sanctions List, EU Sanctions Map, FATF Black/Grey Lists, Transparency International Corruption Perceptions Index.

8. Contact Information

For questions, contact:

- Compliance Department, Horizonix Corp N.V.
- Email: legal.Horizonix.corp@gmail.com + Compliance@ecorpp.com

9. Policy History

Version	Date	Approved By
1.0	September 11, 2024	Ecorpp Management N.V., Director 
2.0	May 05, 2025	Ecorpp Management N.V., Director 
3.0	July 04, 2025	Ecorpp Management N.V., Director 
4.0	January 09, 2026	Ecorpp Management N.V., Director 

10. Policy URL

Available at:

<https://vashbet.com/page/aml-and-kyc-policy>

and

<https://gravira.com/page/aml-and-kyc-policy>

Signed This of January 9, 2026

A handwritten signature in black ink, consisting of a stylized 'D' followed by a horizontal line.

Director: Ecorpp Management N.V.

Appendix 1

Afghanistan
Aland Islands
American Samoa
Angola
Anguilla
Antarctica
Antigua and Barbuda
Barbados
Belize
Benin
Bhutan
Bonaire (including Sint Eustatius and Saba)
Bouvet Island
British Indian Ocean Territory
Burundi
Cape Verde
Central African Republic
Chad
Cocos (Keeling) Islands
Cook Islands
Comoros
Congo, Democratic Republic
Republic of Congo
Crimea
Cuba
Curacao
Djibouti
Equatorial Guinea
Eritrea
Fiji
French Guyana
French Polynesia
French Southern Territories
Gabon
Gambia
Greece
Grenada
Guadeloupe
Guam

Guinea
Guinea Bissau
Guyana
Haiti
Heard Island and McDonald Islands
Holy See (Vatican City State)
Iran
Iraq
Ivory Coast (Côte d'Ivoire)
Kiribati
Kosovo
Kyrgyzstan
Lao People's Democratic Republic
Lebanon
Liberia
Libya
Macao
Malawi
Mali
Marshall Islands
Martinique
Mauritania
Mayotte
Micronesia, Federated States of
Montserrat
Myanmar
Nauru
New Caledonia
Niger
Niue
Norfolk Island
North Korea
Northern Mariana Islands
Palau
Palestinian Territory
Papua New Guinea
Pitcairn
Puerto Rico
Rwanda
Saint Barthelemy
Saint Helena
Saint Kitts and Nevis
Saint Lucia

Saint Martin
Saint Pierre and Miquelon
Saint Vincent and the Grenadines
Sao Tome E Principe
Seychelles
Sint Maarten
Sierra Leone
Solomon Islands
Somalia
South Georgia and the South Sandwich Islands
Sudan (North and South)
Suriname
Svalbard and Jan Mayen
Syria
Tajikistan
Temporarily occupied territories of Ukraine
Timor Leste
Togo
Tokelau
Tonga
Turkmenistan
Turks and Caicos Islands
Tuvalu
United States of America
United States Minor Outlying Islands
US Virgin Islands
Uzbekistan
Vanuatu
Venezuela
Wallis and Futuna
Western Sahara
Western Samoa
Yemen
Zimbabwe