

Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy - SUVYD B.V.

Last Updated: 01.06.2025

Introduction

SUVYD B.V. is dedicated to maintaining the highest standards of security, transparency, and integrity across all of its activities. As a licensed online gaming operator under the laws of Curaçao, we implement strict measures on Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and the prevention of financing the proliferation of weapons of mass destruction (FP). These measures are designed to safeguard our players (hereinafter also referred to as users or customers) and to ensure full compliance with all applicable legal and regulatory requirements, including but not limited to:

- The AML/CFT Regulations issued by the Curaçao Gaming Authority (CGA);
- The National Ordinance on the Reporting of Unusual Transactions (NORUT);
- The National Ordinance on Identification when Rendering Services (NOIS);
- The Kingdom Sanctions Act (Rijkssanctiewet);
- The Sanctions National Ordinance;
- The Financial Action Task Force (FATF) 40 Recommendations.

This Policy establishes the framework by which SUVYD B.V. ensures that only verified and legitimate users are granted access to our services, while also protecting the integrity of our platform and maintaining compliance with international standards.

Purpose of the Policy

This Policy has been developed to ensure SUVYD B.V.'s compliance with applicable Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) obligations and to safeguard the integrity of its gaming platform. Its objectives are to:

- Prevent the use of the platform for illicit financial activities, including money laundering, terrorist financing, or the financing of weapons proliferation;
- Ensure that all player funds originate from lawful sources and are utilized strictly in accordance with applicable laws and the platform's rules;
- Apply risk-based customer identification, verification, and due diligence procedures proportionate to the risk profile of each player;
- Maintain compliance with Curaçao's AML/CFT regulatory framework, including the AML/CFT Regulations, NORUT, NOIS, as well as international standards such as the FATF Recommendations;
- Protect SUVYD B.V.'s players, systems, and reputation by identifying, mitigating, and reducing risks related to fraud, abuse, and financial crime.

Business Risk Assessment (BRA)

SUVYD B.V. maintains a documented Business Risk Assessment (BRA) in accordance with the AML/CFT Regulations issued by the Curaçao Gaming Authority.

The BRA is reviewed at least annually and whenever there are material changes to the business model, products, payment methods, or geographic exposure.

The Business Risk Assessment evaluates the following risk categories:

- Product Risk – online casino, sportsbook, remote gaming services, cryptocurrency transactions;
- Geographic Risk – customers from high-risk or FATF-identified jurisdictions;

- Customer Risk – high-value players, PEPs, non-residents;
- Delivery Channel Risk – non-face-to-face onboarding;
- Payment Method Risk – crypto assets, e-wallets, prepaid instruments.

Each risk category is assessed as Low, Medium, or High, and appropriate mitigation measures are applied, including enhanced monitoring, transaction limits, and Enhanced Due Diligence (EDD) where necessary.

The Business Risk Assessment is formally documented, approved by senior management, and retained as a standalone internal compliance document. The results of the BRA are made available to the Curaçao Gaming Authority upon request.

Definitions

Money Laundering, Terrorist Financing, and Financing of Proliferation (ML/TF/FP): Refers to money laundering, terrorist financing, and proliferation financing offenses as defined under the Penal Code of Curaçao.

Terrorist Financing (TF): The act of providing or collecting funds with the intention that they be used, or in the knowledge that they will be used, for terrorist purposes, regardless of whether the funds originate from lawful or unlawful sources.

Know Your Customer (KYC): The process of identifying and verifying the identity of a customer prior to, or during, the establishment of a business relationship. This includes the collection of personal data, verification of supporting documents, sanctions and PEPs screening, and assessment of the customer's intended activity.

Customer Due Diligence (CDD): The set of measures applied to identify and verify customers, evaluate their risk level, and ensure compliance with AML/CFT regulations.

Politically Exposed Person (PEP): An individual who currently holds, or has previously held, a prominent public function, as well as their immediate family members and close associates.

Sanctions Screening: The process of verifying customers against relevant international and national sanctions lists, including but not limited to UN, EU, and OFAC lists.

FIU: The Financial Intelligence Unit Curaçao, responsible for receiving, analyzing, and disseminating reports of unusual or suspicious transactions.

Scope of Application

This Policy applies to:

- All players registering on the SUVD B.V. platform;
- Any player making deposits or withdrawals;
- All operational, customer-facing, and KYC/AML compliance staff;
- Third-party service providers, including KYC, risk management, and payment processing partners, acting on behalf of SUVD B.V.

Age and Jurisdiction Restrictions

SUVD B.V. is committed to adhering to all applicable age restrictions and jurisdictional access requirements in line with Curaçao licensing regulations and international best practices. Specifically:

Minimum Age Requirement: Access to the platform is strictly restricted to individuals aged 18 years or older. As part of the registration and verification process, SUVD B.V. collects and validates each player's date of birth and supporting identification documents to confirm eligibility. Where local legislation prescribes a higher minimum age for gambling, the higher threshold shall apply. Accounts found to belong to underage users will be terminated, and any associated balances may be forfeited in accordance with this Policy.

Prohibited Jurisdictions: Players residing in, or attempting to access the platform from, high-risk or restricted jurisdictions are strictly prohibited from using our services. This includes countries and territories that are:

- Subject to comprehensive international sanctions (UN, EU, OFAC);
- Identified by the FATF as high-risk jurisdictions subject to a call for action;
- Restricted under Curaçao Gaming Authority (CGA) regulations;
- Explicitly listed on SUVYD B.V.'s internal Prohibited Countries List.

Technical Access Controls: SUVYD B.V. deploys technical measures to restrict access from prohibited jurisdictions, including but not limited to:

- Geo-IP blocking mechanisms;
- VPN and proxy detection tools;
- Restrictions on payment methods linked to unsupported jurisdictions.

These controls are subject to regular review and updates. Any attempt by players to circumvent such restrictions may result in account suspension, limitation, or closure under this Policy.

Account Registration

To register and operate a player account with SUVYD B.V., users are required to complete the full onboarding process by providing the following mandatory information:

- Full legal name;
- Date and place of birth;
- Permanent residential address;
- Nationality;
- Valid and accessible email address;
- Mobile phone number;
- Identity reference number (where applicable);
- Preferred account currency and a secure password.

Upon submission of the registration form, the player will receive a verification email containing an activation link. Access to the platform, including the ability to deposit funds and participate in gaming activities, is only granted after successful email verification.

SUVYD B.V. reserves the right to request additional supporting documentation in order to verify the accuracy of the information provided during the registration process. Any inconsistencies or failure to provide required information may result in account restrictions, suspension, or refusal to onboard the user.

Customer Acceptance Policy (CAP)

SUVYD B.V. shall not establish or maintain a business relationship with:

- Individuals or entities subject to international sanctions;
- Persons located in prohibited or FATF black-listed jurisdictions;
- Anonymous or fictitious persons;
- Customers using third-party payment instruments;
- Customers refusing to provide required identification documentation;
- Persons reasonably suspected of involvement in criminal activity.

High-risk customers, including Politically Exposed Persons (PEPs) and customers from high-risk jurisdictions, require senior management approval prior to onboarding or continuation of the relationship.

Know Your Customer (KYC) and Identity Verification

SUVYD B.V. applies Know Your Customer (KYC) procedures in accordance with Curaçao AML/CFT Regulations to verify the identity of its players and ensure full compliance with applicable legal obligations.

Identity verification may also be requested at any time at the discretion of SUVYD B.V. in order to maintain the integrity of a player's profile and protect the platform.

Only verified players are granted full account functionality, including access to financial transactions. Failure to complete KYC may result in restricted access or account suspension.

Required Documents

Under Curaçao AML/CFT Regulations, players are required to provide the following documents to complete the identity verification process:

1. **Proof of Identity.** A clear, color image or scan of one of the following government-issued photo IDs:
 - Passport (photo page);
 - National identity card (front and back);
 - Driver's license (front and back);
 - Residency card (where applicable).

In addition, a selfie or a photo of the player holding the submitted document next to their face is required to confirm authenticity and to ensure that the document belongs to the person registering the account. The photo must clearly display the player's face and the document without glare, blur, or obstructions.

2. **Proof of Residential Address.** A document issued within the last six (6) months displaying the player's full name and current residential address. Accepted documents include:
 - Utility bill (electricity, water, gas);
 - Bank statement;
 - Lease agreement.
3. **Document Standards.** All documents submitted must:
 - Be in color (black-and-white scans are not accepted);
 - Be legible and unaltered;
 - Show all edges and corners;
 - Be free of glare, blur, or obstructions.
4. **Additional Documentation.** SUVYD B.V. reserves the right to request additional information at any time, including but not limited to:
 - Proof of ownership of payment methods used;
 - Source of Funds (SoF) or Source of Wealth (SoW) documentation;
 - Notarized or certified copies of documents, where necessary for compliance purposes.

Failure to provide complete, accurate, and acceptable documentation may result in delayed verification, or account restrictions.

Verification of Payment Methods

To ensure transparency, ownership, and lawful use of funds, SUVYD B.V. requires that all financial transactions on the platform adhere to the following principles:

- **Personal Use Only.** Players are permitted to use only payment instruments (e.g., bank accounts, credit/debit cards, e-wallets) that are registered in their own name. The use of third-party or jointly held accounts is strictly prohibited.

- **Deposit and Withdrawal Matching.** Where technically feasible, withdrawals must be processed through the same payment method that was originally used for deposits. If this is not possible, the alternative method must also be verified and confirmed to be owned by the player.
- **Cash Transactions Prohibited.** SUVYD B.V. does not accept or issue funds in physical cash. All deposits and withdrawals must be conducted through online, traceable, and regulated financial channels.
- **Documentation Requirements.** The Company may request supporting documents to confirm payment method ownership.

Failure to comply with payment verification requirements may result in transaction denial, account restrictions, or suspension until verification is successfully completed.

Customer Due Diligence (CDD)

SUVYD B.V. applies a risk-based Customer Due Diligence (CDD) framework to establish and verify the identity and legitimacy of all players. The scope and depth of CDD depend on the nature of the player's activity and their assessed risk profile.

- All players are subject to ongoing monitoring.
- Risk classifications may be reassessed and updated over time.
- SUVYD B.V. reserves the right to request additional documentation or information at any stage of the player relationship.

Mandatory CDD Threshold

In accordance with the AML/CFT Regulations, full Customer Due Diligence must be completed when cumulative deposits, single transactions, or linked transactions reach NAf 4,000, regardless of the assigned customer risk level.

No further deposits or withdrawals shall be permitted until verification is successfully completed.

Customer Risk Assessment (CRA)

Each customer is assigned a documented risk rating at onboarding based on:

- Country of residence;
- PEP status;
- Transaction volume;
- Payment methods used;
- Behavioral indicators;
- Source of funds risk.

Customers are classified as Low Risk, Standard Risk, or High Risk.

Risk classification is reviewed annually or upon trigger events, including unusual transactions, cumulative transaction thresholds, or material profile changes.

Risk classification is documented in the customer profile and retained in accordance with record-keeping requirements. The risk rating shall be made available to the Curaçao Gaming Authority upon request.

Politically Exposed Persons (PEPs)

SUVYD B.V. identifies and evaluates whether a player qualifies as a Politically Exposed Person (PEP) or is closely associated with a PEP, in line with Curaçao AML/CFT requirements.

Players designated as PEPs are subject to Enhanced Due Diligence (EDD) measures, which may include:

- Additional and enhanced verification procedures;
- Senior management approval prior to onboarding or continuing the relationship;
- More frequent and detailed reviews of the business relationship.

PEP status is monitored on an ongoing basis, and controls are applied to ensure the relationship remains within the Company's risk tolerance and legal obligations.

Beneficial Ownership Rules

Where a customer is a legal entity or where ownership or control indicators are identified, SUVYD B.V. shall identify and verify the beneficial owner. This requirement applies to corporate customers, business partners, and any legal entities entering into a business relationship with SUVYD B.V.

A beneficial owner is defined as a natural person who:

- Owns 25% or more of the shares; or
- Exercises control over the entity.

Verification includes corporate registry extracts, ownership structure documentation, and identification of controlling individuals.

Changes in ownership must be monitored and verified on an ongoing basis.

Re-Verification and Monitoring

SUVYD B.V. reserves the right to request updated or additional documentation from players in support of ongoing compliance with verification requirements.

Until the requested documentation is reviewed and approved, access to certain account features — including deposits, withdrawals, and gameplay — may be temporarily restricted.

This process ensures that player information remains accurate and up to date, supporting the Company's continuing AML/CFT obligations.

Ongoing Monitoring

SUVYD B.V. conducts ongoing monitoring of all player accounts throughout the duration of the business relationship in order to ensure compliance with AML/CFT regulations.

Monitoring activities include:

- Periodic reviews of submitted documents to confirm their validity and accuracy;
- Reassessment of player risk profiles based on behavioral patterns, transaction activity, or jurisdictional exposure;
- Re-verification when changes in risk, player profile, or regulatory requirements warrant it.
- These measures ensure continuous compliance and the timely identification of potential risks.

Transaction Monitoring

SUVYD B.V. employs a robust transaction monitoring system, which integrates both automated tools and manual oversight, to detect unusual or suspicious activity that may be inconsistent with a player's profile or platform rules.

All monitoring activities are carried out in line with Curaçao AML/CFT obligations and industry best practices, ensuring the early identification and mitigation of financial crime risks.

Internal Reporting and Suspicious Transaction Reporting (STR)

Employees must immediately report any suspicious activity to the Compliance Officer.

The Compliance Officer assesses the information and, where required, submits a report to the FIU Curaçao in accordance with NORUT.

Tipping-off is strictly prohibited.

Linked Transactions and Structuring Detection

SUVYD B.V. aggregates transactions where multiple operations appear linked within a 24-hour or 7-day period.

Monitoring systems detect:

- Structuring of deposits below NAF 4,000;
- Smurfing patterns;
- Multiple accounts linked by IP address, device ID, or payment method;
- Rapid deposit-withdrawal patterns inconsistent with gaming activity.

Suspicious linked transactions trigger enhanced review and, where appropriate, reporting to the FIU Curaçao.

Where transactions are determined to be artificially structured to avoid regulatory thresholds, such activity shall be treated as suspicious.

Sanctions Compliance

SUVYD B.V. performs mandatory sanctions screening on all players in line with Curaçao AML/CFT legislation and international obligations. Players are screened against relevant global sanctions and watchlists, including but not limited to:

- United Nations Security Council (UNSC);
- European Union (EU);
- U.S. Office of Foreign Assets Control (OFAC);
- Other relevant regional or national authorities.

If a player is identified as sanctioned or associated with a sanctioned individual or entity, the account may be blocked, suspended, or restricted in accordance with applicable laws and regulations.

Data Retention

SUVYD B.V. ensures that all records required under AML/CFT legislation are retained in accordance with regulatory requirements. This includes:

- Identification and verification records;
- Submitted KYC documentation;
- Records of financial transactions;
- Compliance-related communications and reports.

All records are stored securely and retained for a minimum of five (5) years following the termination of the business relationship, or for up to ten (10) years if required by the Financial Intelligence Unit (FIU) Curaçao or by applicable legal process.

Independent AML Audit

SUVYD B.V. shall conduct an independent AML review at least annually.

The review shall be performed by a qualified and independent party and shall assess the effectiveness of the Company's AML framework, transaction monitoring systems, and risk assessments.

Findings shall be documented and reported to senior management. Remediation measures shall be tracked and implemented without undue delay.

The independent reviewer must not be involved in the day-to-day AML operations of the Company.

Tailoring and Continuous Improvement

SUVYD B.V. maintains a dynamic and adaptive AML/CTF compliance framework that is regularly reviewed and updated to ensure continued alignment with:

- Legislative and regulatory developments in Curaçao and internationally;
- Operational changes, including new products, technologies, or customer interaction models;
- Emerging risks identified through external sources such as FATF guidance, FIU advisories, or industry best practices;
- Findings from internal reviews, independent audits, and feedback from senior management.

The AML and KYC Policy, along with related procedures and control mechanisms, are reviewed at least annually, and more frequently when material changes in risk exposure, business operations, or regulatory requirements occur.

This proactive approach ensures that SUVYD B.V.'s compliance framework remains effective, risk-proportionate, and responsive to the evolving AML/CTF environment.

AML Training

SUVYD B.V. ensures that all relevant employees receive AML/CTF training upon hiring and annually thereafter. Training covers regulatory obligations, risk indicators, suspicious activity detection, and internal reporting procedures. Training attendance is documented and retained.

Sanctions for Non-Compliance

SUVYD B.V. enforces a strict compliance regime in accordance with Curaçao AML/CTF regulations. Any failure by a player to comply with verification, due diligence, or other AML/CTF-related obligations may result in corrective or enforcement action, including but not limited to:

- Temporary or permanent suspension of the player's account;
- Blocking of withdrawals and denial of further access to services;
- Termination of the business relationship;
- Submission of a report to the Financial Intelligence Unit (FIU) Curaçao or other competent authority;
- Other legal, regulatory, or administrative measures as may be applicable under Curaçao law.

SUVYD B.V. reserves the right to apply such measures at its sole discretion whenever it deems necessary to ensure compliance with its legal obligations and to safeguard the integrity of its platform.

Payout Management

SUVYD B.V. processes withdrawals in accordance with regulatory requirements and internal AML/CTF controls. To ensure the legitimacy of outgoing transactions, the following conditions apply:

- Withdrawals will only be processed after successful verification of the player's identity and payment method ownership;

- Payouts must, where technically feasible, be returned to the same source of funds used for deposit;
- Any wagering or promotional requirements must be fully satisfied before withdrawal (where applicable);
- Deposited funds must be used exclusively for genuine gaming activity and not for purposes inconsistent with the platform's fair use policy.

SUVYD B.V. reserves the right to delay or deny payout requests if verification is incomplete, discrepancies are detected, or additional information is required. Withdrawals to third-party or unverified accounts are strictly prohibited.

Player Responsibilities

To maintain a compliant, fair, and secure gaming environment, all players of SUVYD B.V. are expected to:

- Provide complete, accurate, and up-to-date personal and contact information during registration and throughout the account lifecycle;
- Use only their own identity and financial instruments to access and transact on the platform;
- Respond promptly to any verification or information requests issued by the Company;
- Maintain only one registered account per person and refrain from creating duplicate or secondary accounts;
- Refrain from any attempt to bypass verification, deposit, or bonus restrictions through multi-accounting, use of false credentials, or other fraudulent means.

Failure to meet these responsibilities may result in corrective measures, including account suspension or closure, reversal of bonuses or winnings, or other restrictions in line with the Company's Terms and Conditions and AML/CFT obligations.

Customer Communication

SUVYD B.V. prioritizes open communication and transparency with players regarding compliance requirements. The Company:

- Notifies players promptly when verification is required;
- Provides clear guidance on required documentation and acceptable submission formats;
- Offers dedicated customer support for all compliance-related queries.

Players are encouraged to cooperate proactively and contact support with any questions or concerns regarding verification or compliance.

Data Protection and Confidentiality

SUVYD B.V. ensures the integrity, confidentiality, and security of all sensitive information collected under AML/CFT obligations.

- **Encryption and Secure Storage:** All client information, including KYC records and transaction logs, is encrypted and securely stored in compliance with applicable data protection regulations.
- **Access Control:** Access to compliance-related information is restricted to authorized personnel only.
- **Incident Management:** The Company maintains an incident response plan to ensure rapid resolution of any data breach and regulatory notification, if required.

Cooperation with Authorities

SUVYD B.V. fully cooperates with the Financial Intelligence Unit (FIU) Curaçao, as well as other competent regulatory, supervisory, or law enforcement authorities, as required by law.

Upon lawful request, the Company may disclose or provide access to relevant information, including but not limited to:

- Know Your Customer (KYC) documentation;
- Transaction and account activity records;
- Risk assessments and monitoring logs;
- Internal compliance communications or findings.

Such cooperation is always conducted in full compliance with legal requirements and with due regard to data protection and confidentiality standards.

The Curaçao Gaming Authority (CGA) shall have unrestricted and immediate access, upon request, to all AML-related documentation, including customer files, transaction records, risk assessments, monitoring logs, and internal reports.

SUVYD B.V. shall provide such information without delay.

Role of the Compliance Officer

SUVYD B.V. has appointed a qualified Compliance Officer responsible for the effective implementation and oversight of the Company's AML/CFT program.

Key responsibilities include:

- Ensuring day-to-day compliance with Curaçao AML/CFT regulations;
- Overseeing CDD, transaction monitoring, and internal reporting procedures;
- Acting as the primary liaison with the FIU and other competent authorities;
- Conducting compliance training for staff and ongoing AML/CFT risk assessments.

The Compliance Officer operates independently of operational teams, reports directly to senior management, and has unrestricted access to all customer and transactional data necessary to fulfil these responsibilities.

Support and Contact

All inquiries are handled confidentially and in accordance with privacy and data protection legislation.

SUVYD B.V. remains fully committed to:

- Promoting responsible gaming and fair play;
- Ensuring strict compliance with regulatory obligations;
- Safeguarding the integrity of its gaming environment and protecting its players.