



SGD TECH N.V. KYC Version 1.1

CompanyRegistrationNo.:169025

Know Your Customer (KYC) Policy

Company: SGD TECH N.V.

Registered Address: Trias Building, Hanchi Snoa 19, Willemstad, Curaçao

Platform: <https://kickwin.io>

Version	Description	Effective date	Approved by	date
1	Initial KYC	02/02/2026	Board of Directors	02/02/2026
1.1	Updated	18/03/2026	Board of Directors	18/03/2026

This KYC Policy has been reviewed and formally approved in accordance with applicable Curaçao laws and regulations.

Approved by (Board of Directors):

Name: Ecorpp Management N.V.

Title: Director

Signature: 

Date: 25/03/2026

Reviewed by (Compliance Officer): Name:

Ms. Eliane Solis Vazquez

Title: Compliance Officer

Signature: 

Date: 24/03/2026

1. Policy Statement

SGD TECH N.V. is committed to preventing money laundering, terrorist financing, and other forms of financial crime by implementing effective Know Your Customer ("KYC") measures.

This KYC Policy establishes the principles governing the identification, verification, and ongoing monitoring of customers and forms an integral part of the Company's overall Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") framework.

The Company applies KYC measures using a risk-based approach, ensuring that controls are proportionate to the level of risk identified.

2. Purpose

The purpose of this Policy is to ensure that SGD TECH N.V.:

- Identifies and verifies the identity of customers prior to, or during, the establishment of a business relationship;
- Understands the nature and purpose of customer activity;
- Assesses and manages customer-specific money laundering and terrorist financing risks;
- Prevents misuse of the Company's platform for illicit or prohibited activities;
- Complies with applicable Curaçao laws and regulatory requirements.

3. Legal and Regulatory Framework

This Policy is established in accordance with, and shall be interpreted in line with, the following:

- National Ordinance for Games of Chance (LOK, PB 2024 no. 157)
- National Ordinance on the Identification when Rendering Services (NOIS, PB 2017 no. 92)
- National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017 no. 99)
- Applicable guidance and requirements issued by the Curaçao Gaming Authority (CGA)
- Reporting obligations to FIU Curaçao



SGD TECH N.V.

CompanyRegistrationNo.:169025

4. Scope and Applicability

All players must be duly registered with the Company prior to accessing or using any gaming services.

Players who have not completed the registration process and provided the required minimum identification information shall not be permitted to play, deposit, wager, or otherwise access the Company's platform.

This Policy applies to:

- All customers of SGD TECH N.V., including players using the platform <https://kickwin.io>;
- All customer onboarding channels, including remote and electronic onboarding;
- All employees, contractors, and third parties involved in customer onboarding, verification, payments, and monitoring.

5. Definitions

For the purposes of this Policy, key terms such as Customer, KYC, Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Politically Exposed Person (PEP), Sanctions, High-Risk Jurisdiction, and Suspicious Activity shall have the same meaning as defined in the Company's AML/CTF Policy.

6. Customer Identification and Verification

6.1 Timing of KYC

Customer identification and verification shall be performed:

- Before a business relationship is established; or
- As soon as practicable thereafter, but no later than when regulatory thresholds or risk-based triggers are met; or
- Whenever doubts arise regarding the accuracy or adequacy of previously obtained customer information.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



6.2 Identification Information

At a minimum, the Company shall obtain the following information from individual customers:

- Full legal name;
- Date of birth;
- Nationality;
- Residential address;
- Contact details;
- Details of a valid identification document.

6.3 Verification Measures

Customer identity shall be verified using reliable and independent source documents, data, or electronic verification tools, which may include:

- Government-issued photo identification documents;
- Proof of address where required;
- Electronic or biometric verification solutions, where applicable.

7. Risk-Based Customer Due Diligence

For customers classified as medium or high risk, the Company shall obtain, at a minimum, the following information:

- (1) information on the nature of and details concerning the customer's business, occupation, or employment;
- (2) information on any additional activities from which the customer derives wealth (including, but not limited to, inheritance or investments);
- (3) the expected source and origin of the funds to be used throughout the business relationship; and
- (4) the anticipated level and nature of activity, including the expected value and frequency of transactions.

For high-risk customers, the above information shall be supported by appropriate documentary evidence and shall be subject to enhanced due diligence and ongoing monitoring.

7.1 Customer Risk Assessment

A Customer Risk Assessment (CRA) shall be conducted at onboarding and updated on an ongoing basis.

The assessment takes into account, at a minimum:

- Customer profile and behaviour;
- Transaction size, frequency, and patterns;



- Payment methods used, including cryptocurrency;
- Geographic risk;
- PEP and sanctions exposure.

Customers shall be classified according to their assessed risk level.

7.2 Standard Customer Due Diligence (CDD)

Standard CDD measures shall be applied to customers assessed as presenting normal or lower risk, in accordance with this Policy and applicable legal requirements.

8. Enhanced Due Diligence (EDD)

In addition to screening conducted at onboarding and on an ongoing basis, the Company shall perform PEP screening within thirty (30) days from the moment a customer reaches the applicable deposit threshold triggering Customer Due Diligence requirements, irrespective of whether such screening has previously been performed.

Enhanced Due Diligence shall be applied where a customer, transaction, or business relationship presents a higher risk of money laundering or terrorist financing, including at a minimum:

- Customers connected to high-risk jurisdictions;
- Politically Exposed Persons (PEPs), their family members, or close associates;
- Crypto-related activity presenting elevated risk, including high-value or complex transactions;
- Unusual or excessive gambling behaviour inconsistent with the customer's known profile or expected activity;
- Any other indicators identified through ongoing monitoring or risk assessment.

EDD measures may include additional verification, enhanced source-of-funds analysis, senior management involvement, and increased monitoring.

9. Politically Exposed Persons (PEPs)

The Company shall identify whether a customer is a PEP, or a family member or close associate of a PEP.

Where a PEP relationship is identified:

- Enhanced Due Diligence shall be applied;
- Source of funds and source of wealth shall be assessed where appropriate;
- Ongoing monitoring shall be enhanced.



SGD TECH N.V.

CompanyRegistrationNo.:169025

10. Sanctions Screening

Customers shall be screened against applicable United Nations (UN) and European Union (EU) sanctions lists at onboarding and on an ongoing basis.

Where a sanctions match is identified:

- The customer account shall be restricted;
- Relevant funds shall be frozen without delay;
- The matter shall be escalated to the Compliance Officer / MLRO;
- Competent authorities shall be notified as required by law.

11. Ongoing Monitoring and Updating of KYC Information

Customer information shall be kept up to date through:

Where a customer reaches the applicable deposit threshold triggering Customer Due Diligence requirements, the Company shall ensure that full identification and verification is completed within a maximum period of thirty (30) days.

Where, upon expiry of this 30-day period, the required CDD/KYC information has not been obtained or cannot be verified:

- the customer account shall be suspended;
- all deposits, wagering activity, and withdrawals shall be blocked;
- no further transactions shall be permitted;
- the account shall be reviewed by the Compliance function; and
- the business relationship shall be terminated where CDD/KYC requirements remain unmet.

The Company shall also assess whether the circumstances give rise to suspicion and whether a report to the Financial Intelligence Unit Curaçao is required.

- Ongoing transaction monitoring;
- Periodic review of customer risk profiles;
- Review upon trigger events, including unusual activity, changes in behaviour, or changes in risk classification.

12. Incomplete, Failed, or Refused KYC

Where required KYC information is not provided or cannot be verified:

- Appropriate restrictions may be applied to the customer account;
- Withdrawals or other services may be suspended;
- The business relationship may be terminated where verification cannot be completed within a reasonable timeframe.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



SGD TECH N.V.

CompanyRegistrationNo.:169025

13. Reliance on Third Parties

Where permitted under NOIS, the Company may rely on third parties to perform certain elements of KYC, provided that:

- The Company has immediate and unrestricted access to all underlying KYC data;
- The third party applies AML/CTF standards equivalent to those required under Curaçao law;
- Ultimate responsibility remains with SGD TECH N.V., regardless of any reliance arrangement.

14. Contact Information

For any questions, clarifications, or matters relating to this Know Your Customer (KYC) Policy, including customer identification, verification, ongoing monitoring, or KYC-related compliance concerns, please contact:

Compliance Officer
SGD TECH N.V.
Trias Building, Hanchi Snoa 19
Willemstad, Curaçao

Attention: Ms. Eliane Solis Vazquez
Title: Compliance Officer
Email: compliance@ecorpp.com

The Compliance Officer / MLRO is responsible for oversight of KYC compliance and acts as the primary point of contact with the Curaçao Gaming Authority (CGA) and FIU Curaçao in relation to KYC matters.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



SGD TECH N.V.

CompanyRegistrationNo.:169025

BOARD RESOLUTION

Approval of Know Your Customer (KYC) Policy

SDG TECH N.V.

(Incorporated in Curaçao)

Registered Address: Trias Building, Hanchi Snoa 19, Willemstad, Curaçao

RESOLUTION OF THE BOARD OF DIRECTORS

The undersigned, being the members of the Board of Directors of SGD TECH N.V. (the "Company"), hereby adopt the following resolutions:

1.

RESOLVED THAT the Board of Directors has formally reviewed and approved the Company's Know Your Customer (KYC) Policy, which establishes the principles and requirements for the identification, verification, and ongoing monitoring of customers.

The KYC Policy forms an integral part of the Company's overall AML/CTF framework and is adopted in accordance with applicable Curaçao laws and regulations, including:

- National Ordinance for Games of Chance (LOK, PB 2024 no. 157);
- National Ordinance on the Identification when Rendering Services (NOIS, PB 2017 no. 92);
- National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017 no. 99);
- Applicable requirements and guidance issued by the Curaçao Gaming Authority (CGA).



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



SGD TECH N.V.

CompanyRegistrationNo.:169025

2. Implementation and Oversight

RESOLVED THAT Senior Management is hereby instructed to ensure the effective implementation of the KYC Policy across the Company's operations.

RESOLVED FURTHER THAT the Compliance Officer / Money Laundering Reporting Officer (MLRO) shall oversee the ongoing application, monitoring, and review of the KYC Policy and report material matters to the Board of Directors.

3. Ultimate Responsibility

RESOLVED THAT the Board of Directors retains ultimate responsibility for compliance with KYC and AML/CTF obligations and shall review the KYC Policy at least annually or upon material changes to applicable laws, regulations, or the Company's business activities.

4. Effective Date

RESOLVED THAT this Resolution shall take effect as of [18 / 03 / 2026].

By order of the Board of Directors

For and on behalf of SGD TECH N.V.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io