



Anti-Money Laundering (AML) Policy

Company: SGD TECH N.V.

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

Platform: <https://kickwin.io>

Version	update	approved by	review date	approved
Version 1	02/02/2026	Board of Directors	02/02/2026	X
Updated to align with CGA / LOK / NOIS/NORUT	03/02/2026	Board of Directors	17/02/2026	Preliminarily approved for upload
Version 1.2 in. FIU threshold of 5000 xcg	17/03/2026	Compliance Director	18/03/2026	Approved after feedback CGA

This AML/CTF 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

1.1 Commitment

This Policy is established in accordance with the National Ordinance for Games of Chance (LOK, PB 2024 no. 157), the National Ordinance on the Identification when Rendering Services (NOIS, PB 2017 no. 92), and the National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017 no. 99), as amended from time to time, and applicable regulations and guidance issued by the Curaçao Gaming Authority (CGA).:

- Identify, assess, and manage ML/TF risks across its products, services, delivery channels, customers, and jurisdictions;
- Conduct appropriate customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring throughout the customer relationship;
- Verify customer identity and determine beneficial ownership and control structures;
- Monitor transactions and customer behavior to detect unusual, suspicious, or potentially illicit activity;
- Escalate, document, and report suspicious transactions or activities in accordance with applicable reporting obligations;
- Screen customers, beneficial owners, and relevant parties against applicable sanctions, PEP, and adverse media lists;
- Maintain accurate records to support regulatory oversight and lawful requests from competent authorities;
- Ensure ongoing staff training, internal controls, and accountability.

Senior management fully supports this policy and is responsible for ensuring that adequate resources, systems, and controls are in place to achieve effective AML/CTF compliance.





SGD TECH N.V. AML Version 1.2

CompanyRegistrationNo.:169025

1.2 Scope and Applicability

This AML Policy applies to all business activities, operations, and personnel of the Company, including but not limited to:

- Customer onboarding, registration, verification, and account management processes;
- All deposit, withdrawal, transfer, bonus, rebate, and payout activities;
- Gaming, betting, and any other transactions involving customer funds;
- Payment processing activities, including fiat and cryptocurrency transactions;
- All departments, including operations, customer support, finance, risk management, compliance, and technology;
- All platforms, systems, and delivery channels operated or controlled by the Company;
- Third-party relationships and outsourced services relevant to AML/CTF compliance, including payment service providers (PSPs), KYC/identity verification vendors, sanctions screening providers, and other critical service partners.

This policy applies to all directors, officers, employees, contractors, and relevant third parties acting on behalf of the Company. Compliance with this policy is mandatory and forms part of the Company's overall governance and internal control framework.

Where multiple regulatory or legal standards apply, the Company shall apply the highest applicable AML/CTF standard.

2. Purpose

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") Policy is to define the principles, controls, and procedures adopted by SGD TECH N.V., a company incorporated in Curaçao with its registered address at Trias Building, Hanchi Snoa 19, Willemstad, Curaçao, operating the online gaming platform accessible at <https://kickwin.io> (the "Company" or the "Platform"), to prevent and mitigate the risks of money laundering, terrorist financing, and other forms of financial crime.





2.1 Legal and Regulatory Requirements

This Policy ensures that the Company complies with all applicable anti-money laundering and counter-terrorist financing laws, regulations, and regulatory guidance relevant to its operations, including but not limited to:

- AML/CTF obligations applicable in Curaçao;
- Requirements, conditions, and guidance issued by the Curaçao Gaming Authority (CGA) and/or other competent supervisory bodies;
- Applicable international standards and best practices, including those issued by the Financial Action Task Force (FATF);
- Applicable sanctions, counter-terrorism, and financial crime prevention measures imposed by competent authorities.

The Policy provides a structured internal framework to meet statutory obligations relating to customer due diligence, transaction monitoring, record keeping, and the identification and reporting of suspicious activities.

2.2 Business and Operational Risk Management

The Policy is designed to support the Company's business objectives by ensuring that the Platform is not misused for illicit purposes and that financial crime risks are effectively managed. It establishes a risk-based approach to AML/CTF, taking into account:

- The nature of the Company's online gaming and betting services;
- Customer profiles, behaviors, and transactional patterns;
- Payment methods, including fiat and cryptocurrency transactions;
- Geographic exposure and cross-border activity;
- Relationships with payment service providers, game providers, and other third parties.

By implementing proportionate and effective controls, the Company aims to minimize financial, operational, legal, and reputational risks.





2.3 Governance, Internal Controls, and Accountability

This Policy serves as a cornerstone of the Company's internal governance framework by:

- Defining clear AML/CTF objectives and compliance expectations;
- Supporting consistent application of AML/CTF measures across all departments and systems;
- Establishing accountability for directors, senior management, employees, and relevant third parties;
- Ensuring timely escalation and appropriate handling of suspicious or unusual activities.

2.4 Protection of License, Reputation, and Stakeholders

The Policy is intended to protect the Company's gaming license, business continuity, and reputation by:

- Reducing the risk of regulatory enforcement actions, fines, license suspension, or revocation;
- Maintaining the confidence of regulators, payment service providers, banks, business partners, and customers;
- Demonstrating the Company's commitment to integrity, transparency, and responsible business conduct.

2.5 Continuous Compliance and Framework Enhancement

This Policy provides the basis for ongoing monitoring, periodic review, and continuous improvement of the Company's AML/CTF framework, ensuring it remains effective and aligned with:

- Changes in applicable laws and regulatory expectations;
- Evolving money laundering and terrorist financing typologies;
- Changes to the Company's products, services, technologies, and geographic reach.





SGD TECH N.V. AML Version 1.2

CompanyRegistrationNo.:169025

2.5 Appointment of Compliance Officer / MLRO

SDG TECH N.V. hereby appoints Ms. Eliane Solis Vazquez as the Company's Compliance Officer, who also performs the function of Money Laundering Reporting Officer (MLRO).

The Compliance Officer / MLRO is responsible for overseeing the implementation and effectiveness of the Company's Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") framework in accordance with applicable Curaçao laws and regulations, including the National Ordinance for Games of Chance (LOK, PB 2024 no. 157), the National Ordinance on the Identification when Rendering Services (NOIS, PB 2017 no. 92), and the National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017 no. 99).

2.6 Board of Directors and Senior Management Responsibilities

The Board of Directors and Senior Management of SDG TECH N.V. are responsible for ensuring effective compliance with applicable anti-money laundering and counter-terrorist financing ("AML/CTF") laws and regulations.

Board of Directors

The Board of Directors shall:

- Formally review and approve this AML/CTF Policy and any material amendments thereto;
- Formally review and approve the Business Risk Assessment (BRA);
- Review the identified inherent and residual AML/CTF risks arising from the Company's business activities;
- Formally accept residual AML/CTF risk following the implementation of mitigating controls, or require additional measures where such risks exceed the Company's risk appetite;
- Approve the appointment of the Compliance Officer / MLRO and ensure that the function has sufficient authority, independence, and access to information;
- Receive periodic AML/CTF reports from the Compliance Officer / MLRO, including information on suspicious transaction reporting, material issues, and compliance deficiencies.

All approvals and risk acceptance decisions shall be documented through Board resolutions and/or Board meeting minutes.





2.7 Senior Management

Senior Management shall:

- Implement the AML/CTF Policy and Board-approved controls in day-to-day operations;
- Ensure that adequate resources, systems, and procedures are in place to comply with AML/CTF obligations;
- Support the effective functioning of the Compliance Officer / MLRO;
- Escalate material AML/CTF risks, incidents, or deficiencies to the Board of Directors without undue delay.

3. Audience

This Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) Policy applies to all individuals and entities involved in, or acting on behalf of, SGD TECH N.V., including those supporting or operating the online gaming platform <https://kickwin.io>.

The Policy applies to the following stakeholders:

3.1 Directors and Senior Management

All directors, officers, and members of senior management are subject to this Policy and are responsible for:

- Setting the tone from the top with respect to AML/CTF compliance;
- Ensuring that adequate resources, systems, and controls are in place;
- Supporting the effective implementation and enforcement of this Policy.





3.2 Contractors and Subcontractors

All contractors, consultants, freelancers, and subcontractors engaged by the Company whose activities relate to the Company's operations, systems, or customers are required to comply with this Policy to the extent relevant to their roles and responsibilities.

3.3 Third-Party Service Providers and Suppliers

This Policy applies, where relevant, to third-party service providers and suppliers engaged by the Company, including but not limited to:

- Payment service providers (PSPs) and payment processors;
- Cryptocurrency payment and wallet service providers;
- KYC, identity verification, and sanctions screening providers;
- Game providers, aggregators, and platform technology partners;
- Compliance, audit, and professional service providers.

The Company expects such third parties to maintain AML/CTF standards that are consistent with applicable laws and regulatory expectations and, where appropriate, to cooperate with the Company in meeting its AML/CTF obligations.

3.4 Agents, Representatives, and Business Partners

Where applicable, this Policy applies to agents, affiliates, marketing partners, or other representatives acting on behalf of the Company, particularly where they are involved in customer acquisition, onboarding, or transactions.

3.5 Consequences of Non-Compliance

Failure by any individual or entity subject to this Policy to comply with its requirements may result in disciplinary action, contractual remedies, suspension, termination of engagement, or other appropriate measures, in accordance with applicable laws and contractual arrangements.





SGD TECH N.V. AML Version 1.2

CompanyRegistrationNo.:169025

4. Definitions

For the purposes of this Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) Policy, the following terms shall have the meanings set out below. Unless the context otherwise requires, words in the singular include the plural and vice versa.

4.1 Company

“Company” means SGD TECH N.V., a company incorporated in Curaçao, with its registered address at Trias Building, Hanchi Snoa 19, Willemstad, Curaçao, operating the online gaming platform accessible at <https://kickwin.io>.

4.2 Platform

“Platform” means the online gaming and betting website operated by the Company at <https://kickwin.io>, including all associated domains, mobile applications, systems, and technological infrastructure.

4.3 Money Laundering (ML)

“Money Laundering” means any act or attempted act to conceal, disguise, convert, transfer, acquire, or use property or funds derived from criminal activity in order to make such proceeds appear legitimate.

4.4 Terrorist Financing (TF)

“Terrorist Financing” means the provision, collection, or use of funds or assets, directly or indirectly, with the intention or knowledge that they will be used, in whole or in part, to carry out terrorist acts or to support terrorist organizations or individuals.

4.5 Proliferation Financing (PF)

“Proliferation Financing” means the provision of funds or financial services that contribute to the proliferation of weapons of mass destruction, including nuclear, chemical, or biological weapons, where applicable.





4.6 Financial Crime

“Financial Crime” includes money laundering, terrorist financing, fraud, bribery, corruption, sanctions violations, and any other illegal activity involving financial transactions or misuse of financial systems.

4.7 Customer

“Customer” means any natural or legal person who registers for, accesses, or uses the Company’s Platform, including players, account holders, and any person authorized to act on behalf of an account.

4.8 Beneficial Owner / Ultimate Beneficial Owner (UBO)

“Beneficial Owner” or “Ultimate Beneficial Owner (UBO)” means the natural person(s) who ultimately owns or controls a customer or on whose behalf a transaction is conducted, including any individual who exercises ultimate effective control over a legal person or arrangement.

4.9 Customer Due Diligence (CDD)

“Customer Due Diligence (CDD)” means the measures undertaken by the Company to identify and verify a customer’s identity, understand the nature and purpose of the business relationship, and assess the customer’s risk profile.

4.10 Enhanced Due Diligence (EDD)

“Enhanced Due Diligence (EDD)” means additional and more stringent due diligence measures applied to customers or transactions that present a higher risk of ML/TF, including but not limited to high-risk jurisdictions, high-value transactions, or PEPs.

4.11 Politically Exposed Person (PEP)

“Politically Exposed Person (PEP)” means an individual who is or has been entrusted with prominent public functions, as well as their immediate family members and close associates, in accordance with applicable AML/CTF standards.



**4.12 Sanctions**

“Sanctions” means restrictive measures, including financial sanctions and asset freezes, imposed by competent authorities, international bodies, or governments against designated persons, entities, countries, or regions.

4.13 Suspicious Transaction / Suspicious Activity

“Suspicious Transaction” or “Suspicious Activity” means any transaction or behavior that appears unusual, inconsistent with a customer’s known profile, or indicative of potential money laundering, terrorist financing, or other financial crime.

4.14 Transaction Monitoring

“Transaction Monitoring” means the ongoing review, analysis, and monitoring of customer transactions and behavior to identify unusual or suspicious activity.

4.15 Risk-Based Approach (RBA)

“Risk-Based Approach (RBA)” means the allocation of compliance resources and application of AML/CTF controls in proportion to the level of ML/TF risk identified.

4.16 Know Your Customer (KYC)

“Know Your Customer (KYC)” refers to the processes and procedures used by the Company to identify, verify, and understand its customers as part of CDD and EDD measures.

4.17 Suspicious Transaction Report (STR) / Suspicious Activity Report (SAR)

“Suspicious Transaction Report (STR)” or “Suspicious Activity Report (SAR)” means a report filed with the relevant competent authority in relation to suspected ML/TF or financial crime, in accordance with applicable legal requirements.

4.18 Competent Authority

“Competent Authority” means any governmental, regulatory, supervisory, or law enforcement authority with jurisdiction over the Company’s AML/CTF obligations.





5. Policy Implementation

SDG TECH N.V. implements this Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) Policy through a structured and risk-based framework consisting of documented assessments, defined responsibilities, operational procedures, system controls, and ongoing oversight. The Policy is designed to ensure that identified money laundering, terrorist financing, and proliferation financing risks are effectively prevented and mitigated in a manner proportionate to the Company’s risk exposure.

The Compliance Department is responsible for the overall coordination and oversight of the implementation of this Policy, while operational responsibilities are distributed across relevant departments as described below.

5.1 Business Risk Assessment (BRA)

The Company conducts and maintains a Business Risk Assessment (“BRA”) to identify, assess, and understand the inherent and residual ML/TF risks to which it is exposed.

The BRA considers, at a minimum, the following risk factors:

- Products and services offered by the Company, including online casino and betting activities;
- Types of customers, including individual players and their behavioral patterns;
- Delivery channels, including online platforms, remote onboarding, and electronic payment methods;
- Payment methods, including fiat and cryptocurrency transactions;
- Geographical exposure, including customer location, source of funds, and cross-border activity;
- Technological risks, including system automation, remote access, and emerging technologies.

The BRA evaluates how these factors could be misused for money laundering, terrorist financing, or proliferation financing and assesses the likelihood and impact of such misuse.





Based on the outcome of the BRA, the Company determines:

- The level of ML/TF risk it is prepared to accept;
- The adequacy of existing policies, controls, and procedures;
- Any additional mitigating measures required.

The effectiveness of risk mitigation measures is monitored through transaction monitoring, internal reviews, compliance reporting, and periodic audits.

The BRA is:

- Documented in writing;
- Reviewed whenever material changes occur to the business, operating environment, or regulatory framework;
- Otherwise reviewed at least annually;
- Approved by Senior Management.

A technology risk assessment is conducted prior to the launch of any new product, business practice, delivery mechanism, or material technological change.

5.2 Customer Risk Assessment (CRA)

The Company conducts a Customer Risk Assessment ("CRA") for each customer when establishing a business relationship.

The CRA evaluates the specific ML/TF risk posed by an individual customer, taking into account factors derived from the BRA, including but not limited to:

- Customer identity and residency;
- Source of funds and expected transaction behavior;
- Use of payment methods (including cryptocurrency);
- Transaction size, frequency, and patterns;
- PEP status and sanctions exposure;
- Geographic risk indicators.

The information collected during onboarding and ongoing monitoring is used to assign each customer a risk profile (e.g., low, standard, or high risk).

The CRA is:

- Performed at onboarding;
- Updated on an ongoing basis;
- Reviewed when trigger events occur (e.g., unusual transactions, change in behavior, threshold breaches).





5.3 Customer Acceptance Policy (CAP)

The Company applies a Customer Acceptance Policy ("CAP") to determine whether a customer may be accepted or retained.

Based on the outcome of the CRA, the Company applies the appropriate level of customer due diligence (CDD or EDD). The CAP ensures compliance with obligations relating to:

- Politically Exposed Persons (PEPs);
- Sanctions screening;
- High-risk customer categories.

The CAP identifies customer types that may pose a higher-than-average risk and specifies circumstances under which a customer will be refused or denied access, including but not limited to:

- Inability to satisfactorily verify identity;
- Sanctions or terrorism-related exposure;
- Unacceptable source of funds;
- Failure to provide required documentation.
-

5.4 Customer Due Diligence (CDD)

Timing and Measures

Customer due diligence is conducted:

- At onboarding;
- When cumulative transactions reach XCG 4,000;
- When changes occur to the customer's risk profile;
- On an ongoing basis.

CDD measures include:

- Identity verification;
- Verification of source of funds where required;
- PEP and sanctions screening;
- Enhanced Due Diligence (EDD) for higher-risk customers.





SGD TECH N.V. AML Version 1.2

CompanyRegistrationNo.:169025

Threshold Controls

If a customer reaches XCG 4,000 in cumulative transactions and required documents have not been submitted:

- Account restrictions may be applied;
- Withdrawals may be suspended until verification is completed.

If the required information is not received within 30 days of reaching the threshold:

- The business relationship may be terminated;
- Remaining funds may be handled in accordance with legal and regulatory requirements;
- A report may be filed with the competent authority if appropriate.

Termination of Relationship

Where a business relationship is terminated due to AML/CTF concerns:

- The decision is documented;
- Access to the Platform is revoked;
- Records are retained in accordance with record-keeping requirements.

Sanctions Screening and Asset Freezing

Sanctions screening against UN and EU sanctions lists is conducted:

- At onboarding;
- On an ongoing basis.

If a positive sanctions match is identified:

- Relevant funds are frozen without delay;
- The matter is reported to the competent authorities in Curaçao;
- No transactions are processed until clearance is received.

5.5 Enhanced Due Diligence (EDD)

Enhanced Due Diligence ("EDD") shall be applied where a customer, transaction, or business relationship presents a higher risk of money laundering or terrorist financing.





EDD shall be applied at a minimum in the following circumstances:

- High-Risk Jurisdictions
- Where a customer is resident in, connected to, or conducts transactions involving jurisdictions identified as high-risk or subject to enhanced monitoring by competent authorities or international bodies.
- Politically Exposed Persons (PEPs)
- Where a customer is identified as a Politically Exposed Person, or as a family member or close associate of a PEP.
- Crypto-Related Risks
- Where customers engage in cryptocurrency-related activity that presents elevated risk, including but not limited to:
 - High-value or high-frequency crypto transactions;
 - Use of multiple wallets or rapid movement of funds;
 - Transactions involving anonymity-enhancing technologies or services.
- Unusual Gambling Behaviour
- Where customer gambling behaviour is unusual, excessive, or inconsistent with the customer's known profile, expected activity, or declared source of funds, including patterns indicative of fund circulation or minimal gaming.
- Other High-Risk Indicators
- Where other factors identified through ongoing monitoring or risk assessment indicate a higher level of ML/TF risk.

EDD measures may include additional identity verification, enhanced source of funds analysis, senior management approval, increased transaction monitoring, or other risk-mitigating controls deemed appropriate.

5.6 Ongoing Monitoring

The Company applies ongoing monitoring to ensure customer activity remains consistent with the Company's knowledge of the customer and assessed risk profile.

Monitoring measures include:

- Review of transaction size, frequency, and patterns;
- Identification of unusual or inconsistent behavior;
- Periodic review of customer documentation and risk classification.

Ongoing monitoring is supported by automated systems and manual reviews, with escalation to the Compliance Department where necessary.





5.7 Reliance on Third Parties to Perform Customer Due Diligence

Where permitted by applicable law, the Company may rely on qualified third parties to perform certain elements of customer due diligence, such as identity verification.

Such reliance is subject to:

- Written agreements;
- Assurance that the third party applies AML/CTF standards equivalent to those required by the Company;
- The Company retaining ultimate responsibility for AML/CTF compliance.

5.8 Reporting of Unusual and Suspicious Transactions

The Company recognises that, in addition to suspicion-based reporting obligations under NORUT (PB 2017 no. 99), transactions equal to or exceeding XCG 5,000 shall trigger mandatory review. Any transaction or linked transactions reaching XCG 5,000 must be escalated to the Compliance Officer / MLRO. Where FIU indicators are met, an Unusual Transaction Report (UTR) shall be submitted without delay via goAML.

Thresholds serve as escalation triggers and do not replace suspicion-based reporting obligations.

The Company's obligation to report unusual or suspicious transactions is based on suspicion and not on monetary thresholds, in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017 no. 99).

Monetary thresholds are used solely as risk indicators to trigger enhanced review, analysis, and escalation, and do not in themselves determine whether a report must be filed.

Where, following assessment, a transaction or activity is considered unusual or suspicious, a report shall be submitted regardless of the transaction amount.

5.8.1 FIU Curaçao Reporting Obligations

In accordance with Article 20 NORUT, the Company strictly prohibits tipping-off.

No employee, director, or representative may disclose that a report has been filed, is being reviewed, or may be submitted to FIU Curaçao.

This applies to customers, UBOs, and third parties. Breach may result in disciplinary action and legal consequences.

All unusual or suspicious transactions shall be reported to FIU Curaçao without delay via the goAML reporting system, in accordance with NORUT.

The Company strictly prohibits tipping-off, meaning that no customer or third party shall be informed that a report has been filed or is being considered.

The Company and its staff shall cooperate fully with FIU Curaçao and other competent authorities, including by providing additional information upon lawful request.





5.9 Anti-Money Laundering Compliance Program

The Company maintains a risk-based AML compliance program designed to mitigate ML/TF risks and ensure compliance with applicable laws and regulations.

The AML program includes:

- This AML/CTF Policy and supporting procedures;
- Risk assessments (BRA and CRA);
- Customer due diligence and monitoring;
- Reporting and record keeping;
- Ongoing review and improvement.

The AML program establishes minimum compliance standards across the organization and is reviewed periodically to ensure continued effectiveness.

5.10 Reliance on Third Parties for Customer Due Diligence

Where permitted under the National Ordinance on the Identification when Rendering Services (NOIS, PB 2017 no. 92), the Company may rely on third parties to perform certain elements of customer due diligence.

Such reliance shall be subject to the following conditions:

1. Immediate Access to CDD Data
2. The Company shall have immediate and unrestricted access to all underlying Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) information and documentation obtained by the third party, upon request and without delay.
3. Equivalent AML/CTF Standards
4. The third party must apply AML/CTF measures and standards that are equivalent to those required under applicable Curaçao laws and regulations.
5. Written Reliance Arrangement
6. Reliance on a third party shall be governed by a written agreement defining the scope of reliance, data access rights, and cooperation obligations.
7. Ultimate Responsibility
8. Ultimate responsibility for AML/CTF compliance remains with SGD TECH N.V.
9. Reliance on a third party does not relieve the Company or its Board of Directors of any legal or regulatory obligations.
10. The Company shall conduct ongoing oversight of any third party relied upon to ensure continued compliance with AML/CTF requirements.



**5.11 Sanctions Compliance, Asset Freezing, Escalation and Reporting**

The Company maintains procedures to ensure compliance with applicable financial sanctions regimes and to prevent the provision of services to sanctioned persons, entities, or jurisdictions.

Applicable Sanctions Regimes

The Company applies sanctions measures in accordance with applicable and relevant sanctions regimes, including but not limited to:

- United Nations (UN) sanctions lists;
- European Union (EU) sanctions lists;
- Any other sanctions measures applicable under Curaçao law or required by competent authorities.

Sanctions screening is conducted at onboarding and on an ongoing basis against customers, beneficial owners, and relevant counterparties.

5.11.1 Identification of Sanctions Matches

Where a customer, beneficial owner, or transaction generates a positive or potential sanctions match, the matter shall be treated as a high-risk event and escalated immediately for review.

5.11.2 Freezing of Funds and Transactions

Upon confirmation of a sanctions match:

- All relevant funds and assets shall be frozen without delay;
- No deposits, withdrawals, transfers, wagers, or payouts shall be processed;
- The customer account shall be restricted pending further instructions from competent authorities.

The freezing of funds shall occur prior to any notification to the customer and without tipping-off.



**5.11.3 Escalation and Internal Review**

All sanctions matches shall be escalated immediately to the Compliance Officer / MLRO, who shall:

- Review and assess the match without delay;
- Determine whether the match is confirmed or a false positive;
- Document the assessment and decision-making process.

5.11.4 Reporting to Competent Authorities

Where a sanctions match is confirmed, the Compliance Officer / MLRO shall:

- Notify the relevant competent authorities in Curaçao without delay, as required by applicable laws and regulations;
- Cooperate fully with competent authorities, including by providing additional information upon lawful request;
- Maintain all related records in accordance with record-keeping requirements.

5.11.5 Prohibition of Tipping-Off

The Company strictly prohibits tipping-off.

No customer or third party shall be informed that a sanctions review, freeze, or report has been initiated or submitted.

5.11.6 Record Keeping

All sanctions screening results, freezes, escalations, internal assessments, and communications with competent authorities shall be documented and retained for a minimum period of five (5) years.



**5.12 Incident Reporting**

The Company shall report material incidents in accordance with Article 5.10 of the National Ordinance for Games of Chance (LOK, PB 2024 no. 157).

A material incident includes, but is not limited to, incidents related to:

- Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) compliance;
- System integrity, security breaches, or data protection incidents;
- Significant operational disruptions or control failures;
- Any event that may materially impact regulatory compliance, player protection, or the integrity of the gaming operations.

5.12.1 Reporting Procedure

Material incidents shall be:

- Escalated without delay to the Compliance Officer / MLRO and Senior Management;
- Reported to the Curaçao Gaming Authority (CGA) without undue delay;
- Submitted via the CGA Portal, where applicable, in accordance with CGA reporting requirements.

Documentation and Record Keeping

All incident reports, assessments, communications, and corrective actions shall be documented and retained in accordance with the Company's record-keeping obligations.





6. Compliance and Consequences of Non-Compliance

6.1 Obligation to Comply

All directors, officers, employees, contractors, and third parties subject to this Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") Policy are required to comply fully with its provisions, as well as with all supporting procedures, internal controls, and applicable laws and regulations.

Compliance with this Policy is mandatory and forms an integral part of the Company's governance, risk management, and internal control framework. Failure to comply may expose the Company and individuals to significant regulatory, legal, financial, and reputational risks.

6.2 Internal Disciplinary Consequences

Any breach, circumvention, or failure to adhere to this Policy or related AML/CTF procedures may result in disciplinary action, proportionate to the severity of the violation, including but not limited to:

- Formal warnings or reprimands;
- Mandatory retraining or enhanced supervision;
- Suspension of duties or access rights;
- Termination of employment or contractual engagement;

Disciplinary measures apply regardless of seniority or position and may be imposed even where the breach results from negligence rather than intentional misconduct.





6.3 Legal and Regulatory Consequences

Non-compliance with AML/CTF obligations may result in serious legal and regulatory consequences for the Company and/or individuals, including:

- Administrative fines, penalties, or enforcement actions imposed by competent authorities;
- Criminal liability, where applicable, for individuals involved in money laundering, terrorist financing, or related offenses;
- Mandatory remedial actions, audits, or restrictions imposed by regulators;
- Suspension, limitation, or revocation of the Company's gaming license or other regulatory approvals.

The Company cooperates fully with regulators, supervisory authorities, and law enforcement agencies in connection with any investigation or enforcement action.

6.4 Business and Reputational Risks

Failure to comply with this Policy may result in significant business risks, including:

- Loss of banking relationships or payment service provider (PSP) access;
- Termination or suspension of relationships with key business partners or suppliers;
- Financial losses arising from fraud, fines, or operational disruption;
- Damage to the Company's reputation, customer trust, and market standing.

Such risks may have long-term consequences for the Company's ability to operate, grow, and maintain regulatory approval.

6.5 Reporting of Breaches and Protection Against Retaliation

Employees and relevant stakeholders are required to report any suspected or actual breaches of this Policy promptly to the Compliance Department or designated compliance officer.

The Company prohibits retaliation against any individual who reports concerns in good faith or cooperates with an internal or external investigation.





6.6 Management Responsibility and Remedial Actions

Senior Management is responsible for ensuring that identified deficiencies or breaches are addressed promptly through appropriate remedial actions, which may include:

- Enhancements to policies, procedures, or systems;
- Additional training or staffing;
- Disciplinary measures or contractual enforcement;
- Engagement with regulators or external advisors.

The effectiveness of remedial actions is monitored by the Compliance function and reported to Senior Management as appropriate.

7. Related Information

This Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) Policy should be read in conjunction with the following internal documents, external legal and regulatory frameworks, and supporting guidelines. These materials provide additional guidance and operational detail to support effective implementation of the Company’s AML/CTF obligations.

7.1 Internal Policies and Procedures

The following internal policies, procedures, and supporting documents are maintained by the Company and are subject to periodic review by the Compliance Department:

- Customer Due Diligence (CDD and EDD) Procedures
- Customer Acceptance Policy (CAP)
- Business Risk Assessment (BRA)
- Customer Risk Assessment (CRA)
- Transaction Monitoring Procedures
- Suspicious Activity Identification and Reporting Procedures
- Sanctions, PEP, and Adverse Media Screening Procedures
- Record Keeping and Data Retention Policy
- Employee Training and Awareness Policy
- Responsible Gaming Policy
- Data Protection and Privacy Policy





7.2 Legal and Regulatory Frameworks

This Policy is informed by, and aligned with, applicable legal and regulatory requirements, including but not limited to:

- Anti-Money Laundering and Counter-Terrorist Financing laws and regulations applicable in Curaçao;
- Requirements, rules, and guidance issued by the Curaçao Gaming Authority (CGA);
- Reporting obligations and guidance issued by the Curaçao Financial Intelligence Unit (FIU Curaçao);
- Applicable international sanctions regimes, including those issued by the United Nations (UN) and the European Union (EU).

7.3 International Standards and Guidelines

The Company's AML/CTF framework is further guided by internationally recognized standards and best practices, including:

- Financial Action Task Force (FATF) Recommendations and Guidance;
- Risk-based approach guidance relevant to online gaming and remote customer onboarding.

7.4 External Service Providers and Tools

Where applicable, the Company relies on approved third-party service providers and systems to support AML/CTF compliance, including:

- Identity verification and KYC service providers;
- Sanctions and PEP screening tools;
- Transaction monitoring and risk management systems.

The Compliance Department maintains oversight of these providers and ensures they meet the Company's AML/CTF standards.





7.5 Forms, Templates, and Records

The following forms, templates, and records are used to support AML/CTF processes and are maintained in accordance with record-keeping requirements:

- Customer onboarding and verification forms;
- Risk assessment templates (BRA and CRA);
- Internal suspicious activity escalation forms;
- Training attendance and certification records;
- Compliance review and audit logs.

7.6 Record Keeping and Retention

The Company shall retain all CDD and transaction records in accordance with NOIS (PB 2017 no. 92) and NORUT.

CDD records include identification documents, verification data, UBO information, SOF/SOW, and risk assessments.

Transaction records include deposits, withdrawals, wagers, payment methods, timestamps, and account activity logs.

All records must be retained for a minimum of five (5) years after the end of the relationship or transaction date.

Records must be securely stored, retrievable without delay, and available to FIU Curaçao and CGA upon request.

The Company shall maintain complete, accurate, and up-to-date records in relation to its AML/CTF obligations in accordance with applicable Curaçao laws and regulations.

Retention Period

The following records shall be retained for a minimum period of five (5) years from the date the business relationship ends or the date of the transaction, whichever is later:

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) records, including identification documents, verification data, risk assessments, and supporting information;
- Transaction records, including deposits, withdrawals, transfers, wagers, payouts, and related account activity;
- Unusual Transaction Reports (UTRs) and Suspicious Transaction Reports (STRs), including internal assessments, supporting documentation, and correspondence with FIU Curaçao;
- Records relating to sanctions screening, freezes, and related escalation actions.

Storage and Accessibility

Records shall be stored securely, in a manner that ensures confidentiality, integrity, and





SGD TECH N.V. AML Version 1.2

CompanyRegistrationNo.:169025

availability, and shall be capable of being retrieved without undue delay.

All records shall be made available to the Curaçao Gaming Authority (CGA), FIU Curaçao, or other competent authorities upon lawful request.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



8. Independent AML Audit and Compliance Review

The Company shall ensure that its Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) framework is subject to periodic independent audit or compliance review to assess its effectiveness and compliance with applicable laws and regulatory requirements.

Scope of the Review

The independent audit or compliance review shall, at a minimum, assess:

- Compliance with applicable Curaçao AML/CTF laws and regulations, including LOK, NOIS, and NORUT;
- The effectiveness of the AML/CTF Policy, procedures, and internal controls;
- The adequacy of the Business Risk Assessment (BRA) and Customer Risk Assessment (CRA);
- The effectiveness of customer due diligence, transaction monitoring, sanctions compliance, and reporting processes;
- The governance, independence, and effectiveness of the Compliance Officer / MLRO function.

8.1 Independence and Frequency

The audit or review shall be conducted by an independent and qualified party, which may include external auditors or independent compliance professionals, who are not involved in the day-to-day operation of the Company.

Such audit or review shall be conducted:

- Periodically, and
- At least once every year, or more frequently where required by regulatory developments, material changes to the business, or identified AML/CTF deficiencies.

8.2 Reporting and Remediation

The findings and recommendations arising from the independent audit or compliance review shall be:

- Documented in a written report;
- Provided to Senior Management and the Board of Directors;
- Subject to timely remediation, with corrective actions tracked and implemented where necessary.





9. Contact Information

For any questions, clarifications, or concerns regarding this Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) Policy, or for the reporting of potential breaches, suspicious activities, or compliance matters, please contact:

Compliance Department
SDG TECH N.V.
Trias Building, Hanchi Snoa 19
Willemstad, Curaçao
Email: compliance@ecorpp.com

The Compliance Department is responsible for overseeing AML/CTF compliance, responding to internal and external inquiries, and acting as the primary point of contact with regulators and competent authorities in Curaçao.





SGD TECH N.V. AML Version 1.2

CompanyRegistrationNo.:169025

BOARD RESOLUTION

Approval of AML/CTF Policy, Business Risk Assessment and Acceptance of Residual Risk

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. Approval of AML/CTF Policy

RESOLVED THAT the Anti-Money Laundering and Counter-Terrorist Financing Policy (the "AML/CTF Policy") of the Company is hereby formally reviewed and approved 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).

2. Approval of Business Risk Assessment (BRA)

RESOLVED THAT the Board of Directors has reviewed and approved the Company's Business Risk Assessment (BRA), including the identification and assessment of inherent and residual money laundering and terrorist financing risks arising from the Company's products, services, customers, delivery channels, technologies, and geographic exposure.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io

**3. Acceptance of Residual AML/CTF Risk**

RESOLVED THAT, following the implementation of mitigating controls, the Board of Directors hereby formally accepts the residual AML/CTF risk identified in the Business Risk Assessment as being within the Company's risk appetite.

Where residual risk is deemed unacceptable, the Board directs Senior Management to implement additional mitigating measures.

4. Oversight and Ongoing Review

RESOLVED THAT the Board of Directors retains ultimate responsibility for AML/CTF compliance and shall:

- Receive periodic AML/CTF reporting from the Compliance Officer / MLRO;
- Review material AML/CTF issues, incidents, or deficiencies;
- Ensure that the AML/CTF framework is reviewed at least annually or upon material changes to the business or regulatory environment.

5. Effective Date

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

order of the Board of Directors

Name: _____

Title: Director

For and on behalf of SGD TECH N.V.

