

ANTI-MONEY LAUNDERING POLICY

Kanggiten B.V.

CHANGE HISTORY

Date	Version	Author	Summary
May 2025	1.0	Kanggiten B.V.	New version of ANTI-MONEY LAUNDERING policy

Next Scheduled Review: May 2026

Contact Information:

Name: Everhona Francisca Makaya

Position: Money Laundering Reporting Officer (MLRO)

Phone: +599 9 696 7068

Email: compliance@xcm.cw

Table of Contents

1. Policy statement	4
2. Purpose and Legal framework	4
3. Audience	4
4. Definitions.....	5
5. Policy Implementation.....	6
6. Business Risk Assessment.....	7
6.1 Methodology	7
6.2 Identified Risk Areas and Mitigation Measures.....	7
6.3 Risk Scoring and Categorization	8
6.4 Ongoing review of the Business Risk Assessment	9
7. Due Diligence	10
7.1 Risk-Based Approach	10
7.2 Customer Due Diligence and Information Collected	10
7.3 Ongoing Monitoring.....	11
7.4 Enhanced Due Diligence (EDD)	11
8. Anti-Money Laundering Compliance Program.....	11
8.1 Governance and Oversight.....	11
8.2 Termination procedures	12
8.3 Review and Program Assessment.....	12
9. Money Laundering Reporting Officer	12
9.1 Internal Reporting Procedures	13
10. Compliance and Consequences of Non-Compliance.....	13
10.1 Consequences of Non-Compliance.....	13
10.2 Reporting and Enforcement	14
11. Reporting of Unusual Transactions and Suspicious Activity	14
11.1 Types of Reportable Transactions	14
11.2 Internal Escalation and Reporting to FIU	14
11.3 Record-Keeping	15
11.4 Confidentiality and Non-Tipping Off.....	15
12. Record-Keeping	15
13. Employee Training and Awareness.....	15
13.1 Training Program	15
13.2 Frequency and Scope	16
13.3 Training Records	16

1. Policy statement

This Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) Policy outlines the commitment of Kanggiten B.V., a limited liability company incorporated under the laws of Curacao, with the company number 147119, having registered office at Korporaalweg 10, Willemstad, Curaçao (hereinafter – the Company) to uphold the highest standards of compliance in the prevention of money laundering, terrorist financing, and proliferation financing.

As a B2B aggregator of online games under Curaçao law, the Company acknowledges its regulatory responsibilities and exposure to financial crime risks through business-to-business relationships. While the Company does not interact directly with players or hold customer funds, it implements robust internal controls to ensure it is not misused by third parties for illicit purposes.

This policy applies to all departments, employees, directors, and relevant third parties engaged with the Company, and defines the principles, systems, and procedures in place to detect, prevent, and report potential ML/TF activities. It reflects our risk-based approach, ethical standards, and commitment to cooperating with competent authorities.

2. Purpose and Legal framework

The purpose of this AML/CFT Policy is to establish a structured, risk-based program for identifying, mitigating, and managing the risks of money laundering and terrorist financing specific to the Company's operations as a B2B online casino game aggregator.

The policy ensures that the Company complies with national legislation and anticipated regulatory developments applicable to B2B entities in Curaçao, while also aligning with international standards.

The company is subject to a variety of laws, regulations and guidelines in relation to Anti-Money Laundering (AML) and Countering the Financing of Terrorism, both at the national and international levels, including but not limited to:

- National Ordinance on the Reporting of Unusual Transactions (NOIS)
- National Ordinance on Identification when Rendering Services (NORUT)
- Sanctions National Ordinance
- National Ordinance on Games of Chance (LOK)
- FATF Recommendations
- CFATF Guidelines
- UN Sanctions Regime and EU Sanctions Framework

This framework will be continuously updated to reflect any new obligations issued under the LOK or supervisory guidance from the Curaçao Gaming Control Board (GCB).

3. Audience

This Policy applies to all individuals and entities involved in the operations of Kanggiten B.V., including but not limited to:

- **All Employees:** Every employee, regardless of their role or seniority, is required to understand and adhere to the anti-money laundering and counter-terrorist financing obligations outlined in this policy. This includes developers, compliance officers, finance staff, and senior management.
- **Management and Executive Team:** Responsible for fostering a culture of compliance and for providing adequate resources and oversight to support effective AML/CTF risk management.
- **Appointed MLRO (Money Laundering Reporting Officer):** The designated officer responsible for the implementation, monitoring, and enforcement of the AML program.
- **Contracted Consultants or Advisors:** Any external parties providing legal, regulatory, or operational consulting services related to AML/CTF must act in accordance with this policy.
- **Third-Party B2C Clients (Licensed Casinos):** While the company does not maintain direct interaction with players, it requires that its business partners—licensed B2C operators—comply with recognized AML/CTF frameworks. The company conducts due diligence on all such clients before engagement.
- **Technology Partners and Service Providers:** If involved in transactional data processing, identity management, or integration services, these parties must follow the relevant clauses of this policy and ensure no system vulnerabilities are exploited for ML/TF purposes.

All individuals and entities within this scope are required to understand and adhere to the provisions of this policy and to act in accordance with the risk-based procedures adopted by the Company. Employees and relevant third parties will receive appropriate training and guidance to fulfill their obligations under this policy and applicable AML/CFT laws and regulations.

Failure to comply with this policy may result in disciplinary measures, contract termination, or reporting to regulatory authorities.

4. Definitions

For the purpose of this policy, the following terms are defined as follows:

AML (Anti-Money Laundering)	A set of procedures, laws, and regulations designed to stop the practice of generating income through illegal actions, including disguising the origins of criminal proceeds.
CFT (Countering the Financing of Terrorism)	Measures aimed at detecting, preventing, and disrupting the financing of terrorist activities.
Proliferation Financing	The act of providing funds or financial services used for the manufacture, acquisition, possession, development, transport, transfer, or use of nuclear, chemical or biological weapons and their means of delivery, in contravention of national laws or international obligations.
Money Laundering (ML)	The process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions.
Terrorist Financing (TF)	The provision or collection of funds with the intention or knowledge that they will be used to carry out terrorist acts.
MLRO (Money Laundering Reporting Officer)	The designated person within the Company responsible for ensuring compliance with AML/CFT obligations, overseeing internal controls, and serving as the primary liaison with the Financial Intelligence Unit (FIU) Curaçao.

FIU (Financial Intelligence Unit Curaçao)	The national authority responsible for receiving, analyzing, and disseminating reports of unusual and suspicious transactions in Curaçao.
Due Diligence	The process by which the Company evaluates and verifies the identity, legitimacy, ownership structure, and risk profile of its potential business clients—such as casino operators or licensed gaming platforms—prior to establishing or continuing a business relationship.
PEP (Politically Exposed Person)	An individual who is or has been entrusted with prominent public functions and presents a higher risk for potential involvement in bribery or corruption.
Sanctions Lists	Official lists maintained by international or national authorities (e.g., EU, UN, OFAC) that designate individuals, organizations, or countries subject to restrictions due to involvement in criminal activities, terrorism, or proliferation.
Unusual Transaction	A transaction that is inconsistent with the expected behaviour of a customer or partner, or that lacks an apparent lawful purpose, which may indicate ML/TF, or proliferation financing.
Suspicious Activity Report (SAR)	A report submitted to the FIU when there are grounds to suspect that a transaction involves criminal property or is otherwise connected to ML/TF, or proliferation financing.
B2B (Business-to-Business)	A commercial arrangement in which services or goods are provided by one business entity to another, rather than to individual consumers.
the Regulator	The Curaçao Gaming Authority (CGA). The regulator for the entire gaming industry operating in and from Curaçao.
the Company	Kanggiten B.V., a limited liability company incorporated under the laws of Curacao, with the company number 147119, having registered office at Korporaalweg 10, Willemstad, Curaçao
the aggregator	A B2B company that integrates and distributes online gaming content from multiple game developers.

5. Policy Implementation

The implementation of this AML/CFT policy is the responsibility of the Company's senior management under the oversight of the appointed MLRO. The following operational procedures and responsibilities apply:

- Designation of MLRO: The Company has appointed an MLRO responsible for AML/CFT oversight, reporting, and training activities.
- Internal Controls: Internal systems and controls are in place to detect and prevent ML/TF risks in the B2B relationships.
- Onboarding Procedures: B2B clients are subject to risk-based due diligence during onboarding, including identity verification, license validation, and sanctions screening.
- Monitoring: Business partners are monitored on an ongoing basis to detect unusual or suspicious activities.
- Training: Relevant staff receive AML training on risk awareness, internal reporting, and obligations under the law.
- Policy Review: This policy is reviewed annually or in the event of material changes to the business, regulatory framework, or risk exposure.

The MLRO is responsible for ensuring the effective execution of the AML program and reporting obligations to the relevant authorities where applicable.

6. Business Risk Assessment

The Company adopts a risk-based approach (RBA), in line with applicable Curaçao regulations and international standards. The purpose of the business risk assessment (BRA) is to identify, understand, assess, and mitigate the risks the Company may be exposed to in relation to money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

The Company performs regular risk assessments to ensure its AML/CFT controls are proportionate and effective. The BRA is reviewed annually and whenever significant changes occur (e.g., expansion into new markets, onboarding of new clients, or regulatory updates).

6.1 Methodology

The Company's BRA considers the following core risk factors:

- **Product/Service Risk:** Assessment of how the Company's software or content could be misused to facilitate ML/TF by downstream operators.
- **Client Risk:** Evaluation of the licensing, reputation, and jurisdiction of B2B clients. This includes risk-based onboarding and periodic reviews.
- **Geographical risk:** Consideration of the jurisdictions in which B2B partners operate or offer their services, especially where those jurisdictions are designated as high-risk.
- **Delivery channels and distribution methods:** As a digital aggregator, the Company evaluates the risk of remote onboarding or third-party intermediaries involved in service delivery.
- **Reputational and compliance risk:** Evaluation of the Company's potential exposure to reputational damage through association with unethical or non-compliant clients, as well as the risk of enforcement actions due to failure to detect or mitigate ML/TF threats in the value chain.
- **Regulatory obligations:** Review of the regulatory frameworks applicable to the Company and relevant international AML/CFT standards. The Company assesses the adequacy of its policies and procedures in meeting evolving legal requirements, and updates its controls accordingly.

Each risk area is assessed in terms of likelihood and impact, and appropriate mitigation measures are implemented.

6.2 Identified Risk Areas and Mitigation Measures

Risk Area	Key Risks Identified	Mitigation Measures Implemented
Clients (B2B relationships)	- Clients operating without proper licenses - Clients based in high-risk or sanctioned jurisdictions - Clients engaging in activities inconsistent with declared business model	- Onboarding only licensed and regulated clients - Jurisdictional risk screening - KYC/DD performed on all clients - Ongoing monitoring of business relationships

Products and Services	- Use of RNG and gaming services for layering criminal proceeds - Abuse of platform integration to mask illicit activities	- Contractual clauses prohibiting misuse - Technical restrictions on integration - Transaction logs retained and reviewed
Geographic Risk	- Exposure to high-risk or non-cooperative jurisdictions - Cross-border clients with unclear ownership structures	- Use of FATF, EU, UN, CFATF, and GCB country risk lists - Higher due diligence and approval thresholds for such regions
Delivery Channels	- Lack of physical presence increases impersonation/fraud risk - Remote onboarding can obscure beneficial ownership	- Secure onboarding protocols - Verification of business registration, corporate ownership, and licensing documents
Transaction Monitoring	- Large, unusual, or unexplained invoice amounts - Transactions inconsistent with expected business activity	- Internal review of incoming/outgoing payments - Escalation to MLRO for unusual activity - Potential reporting to FIU
Proliferation Financing	- Engaging entities involved in WMD proliferation or under trade restrictions	- Screening against sanctions and watchlists - Refusal of business with entities on proliferation concern lists
Reputational Risk	- Association with fraudulent operators or platforms that accept unregulated traffic	- Media screening and adverse information checks - Rejection of clients with negative media, criminal history, or unresolved regulatory issues
Regulatory Risk	- Non-compliance with AML/CTF requirements set by GCB, NOIS, NORUT, LOK	- Appointment of MLRO - Regular updates of AML policy - Annual compliance and BRA reviews

6.3 Risk Scoring and Categorization

The Company uses a structured risk scoring methodology to classify its clients into risk categories—Low, Medium, or High—based on multiple factors that are evaluated during onboarding and periodically throughout the business relationship.

Risk Scoring Criteria

Each client is assessed across defined risk factors, including but not limited to:

- **Jurisdictional risk:** Whether the client operates in or is incorporated in a country listed by FATF as high-risk or under increased monitoring, or a jurisdiction subject to sanctions.
- **Regulatory status:** The type and credibility of the license held by the client, including whether it is a recognized and regulated B2C operator or an unlicensed entity.
- **Business activity and services:** The nature and complexity of the client's operations (e.g., offering player-facing services or further sublicensing), and whether such activities pose elevated ML/TF risks.
- **Ownership structure:** Transparency of beneficial ownership and the existence of any politically exposed persons (PEPs), sanctioned individuals, or high-risk entities.
- **Transactional behaviour:** Payment practices, revenue size, and any unusual or inconsistent financial flows linked to the Company's services.

- **AML controls and reputation:** The strength of the client's own AML/CTF program, past regulatory history, and reputational indicators.

Each factor is assigned a weighted score. The total risk score determines the client's classification:

Risk Categories

- **Low Risk:** Clients operating in well-regulated jurisdictions with transparent structures and minimal exposure to ML/TF risks. These clients undergo standard due diligence, and their activities are subject to routine review.
- **Medium Risk:** Clients with moderate risk factors, such as operations in countries with evolving regulatory regimes or those with partially opaque structures. Enhanced due diligence may apply during onboarding or periodic reviews, with closer transaction monitoring.
- **High Risk:** Clients presenting significant ML/TF exposure due to risk factors such as operation in high-risk jurisdictions, PEP involvement, or suspicious financial behaviour. These clients are subject to Enhanced Due Diligence (EDD), ongoing monitoring, and approval by senior management.

Ongoing Risk Review

Risk categorization is not static. The Company performs periodic reassessments, triggered by:

- Changes in client ownership, jurisdiction, or regulatory status;
- Internal red flags or adverse media;
- Material changes in the client's use of Company services;
- Updates to regulations.

Based on reassessment results, the Company may escalate or downgrade a client's risk level and apply corresponding due diligence measures.

6.4 Ongoing review of the Business Risk Assessment

The Company recognises that the risk landscape in the gaming industry, especially within the B2B environment, is dynamic. To ensure that its AML/CTF controls remain effective and proportionate to the current threat environment, the Business Risk Assessment (BRA) is subject to a structured and periodic review.

The BRA is reviewed:

- At least annually to reflect changes in the external risk environment, emerging typologies, or updated regulatory expectations;
- Immediately following any significant business developments, including the introduction of new products or services, new markets or jurisdictions, or changes in delivery channels;
- Whenever there is a regulatory update from the Curaçao Gaming Control Board or applicable international standards (e.g. FATF, CFATF).

In addition to the annual review, the BRA will be reassessed when any of the following events occur:

- Launch of a new B2B product, game engine, or software solution;
- Onboarding of clients in new jurisdictions or high-risk sectors;
- A material change in the Company's ownership, corporate structure, or operating model;
- Identification of new ML/TF threats;

- Recommendations issued by regulators or consultants indicating gaps in risk assessment coverage.

7. Due Diligence

As a B2B company, the Company does not maintain direct relationships with individual players. Instead, Due Diligence is applied to all business clients, with the objective of ensuring that services are not provided to entities involved in, or exposed to, money laundering, terrorist financing, or proliferation financing.

7.1 Risk-Based Approach

The Company applies a risk-based Customer Due Diligence (CDD) process prior to entering into or continuing any business relationship with a B2B client. The purpose of CDD is to ensure the Company understands who its clients are, the nature of their business, and the legitimacy of their operations, in order to assess and mitigate potential ML/TF risks.

As part of the onboarding procedure, the Company requires all prospective clients to complete a standardized due diligence form. The submitted form, along with supporting documentation, is reviewed by the AML Compliance team.

The Company verifies the accuracy of the information provided through independent and reliable sources, including company registries, licensing authority records, and open-source checks. The level of due diligence conducted is proportionate to the client's risk rating as determined by the Business Risk Assessment. Clients operating in or serving high-risk jurisdictions, those with weak AML frameworks, or those showing inconsistencies in operations may be subject to closer scrutiny.

No business relationship shall be established or maintained without completing the CDD process to the Company's satisfaction. Incomplete forms or failure to provide required documentation may result in rejection or termination of the relationship.

7.2 Customer Due Diligence and Information Collected

CDD measures are performed:

- Prior to establishing a new business relationship with a client.
- Upon material changes to an existing client's ownership, operational scope, or regulatory status.
- When there are doubts about the veracity or adequacy of previously obtained client data.
- In response to any red flags or indicators of potentially suspicious activity.

Collected information includes (but is not limited to):

- full legal name,
- legal form,
- registration number,
- licensing details,
- registered business address,
- UBO and director identification documents,
- and any other relevant data deemed necessary by the Company's AML function.

Documents are stored securely in digital format, with access restricted to authorised compliance personnel. The Company ensures that all records can be promptly retrieved and provided upon request.

7.3 Ongoing Monitoring

The Company continuously monitors business relationships to ensure that the activities of its clients remain consistent with the initial risk profile. Any significant changes—such as expansion into new jurisdictions, changes in ownership, regulatory action, or unusual service requests—trigger a reassessment. Periodic reviews of client documentation are conducted, and any outdated or incomplete records are updated in a timely manner.

7.4 Enhanced Due Diligence (EDD)

Clients classified as high-risk are subject to Enhanced Due Diligence (EDD) measures. High-risk classifications may result from factors including:

- Operations in or connections with high-risk jurisdictions.
- Ownership by or association with Politically Exposed Persons (PEPs).
- Involvement in activities that pose higher ML/TF exposure.
- Adverse media or negative regulatory history.

EDD measures include, but are not limited to:

- Obtaining additional identification documents or business records.
- Performing background and reputational checks on beneficial owners and directors.
- Requesting detailed information on the source of funds and wealth.
- Requiring senior management approval to enter or continue the relationship.
- Conducting more frequent reviews and intensified monitoring of transactional behaviour.

EDD may be conducted not only at onboarding but also during the course of the relationship when risk factors arise.

8. Anti-Money Laundering Compliance Program

The Company has implemented a risk-based Anti-Money Laundering (AML) Compliance Program designed to prevent the use of its services for money laundering, terrorist financing, or proliferation financing. The program reflects the nature and size of the business, its risk profile, and applicable obligations under Curaçao's regulatory framework and international standards.

8.1 Governance and Oversight

The Company's compliance framework is overseen by Senior Management and implemented by the designated Money Laundering Reporting Officer (MLRO). The MLRO is responsible for the day-to-day execution and maintenance of the AML program, ensuring that internal controls, procedures, and monitoring systems are aligned with regulatory requirements and the Company's risk exposure.

The MLRO is responsible for ensuring that AML/CTF obligations are integrated into the Company's operations and that all relevant employees are adequately trained and informed of their responsibilities. Senior Management maintains overall accountability for the effectiveness of the AML program, supporting a strong compliance culture and ensuring that significant risks, breaches, or regulatory issues are promptly addressed.

8.2 Termination procedures

In line with Curaçao Gaming Control Board requirements, the Company reserves the right to block services and terminate a business relationship if:

- The client fails to provide requested information or documentation.
- The client is identified as high-risk or associated with ML/TF indicators without reasonable explanation.
- The Company reasonably suspects that its services are being misused for criminal purposes.

Such decisions are documented and escalated to the MLRO and, where applicable, reported to the relevant authority.

8.3 Review and Program Assessment

The AML program is subject to regular internal reviews by the Compliance team and periodic assessments to ensure its effectiveness. The MLRO is responsible for reporting findings to senior management, recommending corrective actions, and ensuring timely implementation.

9. Money Laundering Reporting Officer

The Company has appointed a designated Money Laundering Reporting Officer (MLRO), who is responsible for the implementation, oversight, and continual improvement of the Company's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) program.

The MLRO's responsibilities include:

- Designing and maintaining the Company's AML/CTF compliance framework, including policies, and internal controls.
- Regularly reviewing and updating the AML program to ensure alignment with applicable Curaçao regulations, international standards, and internal risk assessments.
- Conducting and coordinating risk assessments to evaluate the Company's exposure to money laundering, terrorist financing, and proliferation financing threats.
- Ensuring that relevant personnel receive AML/CTF training appropriate to their roles, and maintaining training records.
- Reviewing and approving onboarding and continued engagement with higher-risk clients, such as those operating from high-risk jurisdictions or linked to PEPs.
- Overseeing the Company's internal transaction monitoring processes, including the review of flagged activity and the escalation of suspicious transactions.
- Liaising with the Financial Intelligence Unit (FIU) Curaçao and other competent authorities, as necessary.

- Reporting regularly to senior management regarding the effectiveness of the AML/CTF program and any material compliance issues.

9.1 Internal Reporting Procedures

All employees of the Company are required to promptly report any suspected or unusual activity to the MLRO. This includes activity that deviates from a client's known business profile, appears unexplained, or may indicate a breach of AML/CTF obligations.

Reports to the MLRO must be detailed and include all relevant information such as:

- Date and time of the activity
- Parties involved
- Description of the suspicious behavior or transaction
- Supporting documents or communication (where applicable)

The MLRO will review each report, determine whether further investigation is warranted, and decide if a report must be submitted to the FIU Curaçao.

10. Compliance and Consequences of Non-Compliance

The Company is committed to full compliance with all applicable anti-money laundering and counter-terrorism financing (AML/CTF) laws, regulations, and guidelines. This includes adherence to obligations under:

- The National Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS);
- The National Ordinance on the Reporting of Unusual Transactions (NORUT);
- The Landsverordening op de Kansspelen (LOK);
- Relevant guidance issued by the Curaçao Gaming Control Board (GCB) and the Financial Intelligence Unit Curaçao (FIU Curaçao);
- International standards, including those set by the Financial Action Task Force (FATF).

All employees, contractors, and stakeholders of the Company must comply with this AML policy and associated internal procedures. Failure to do so may expose the Company and individuals to regulatory, legal, and reputational risk.

10.1 Consequences of Non-Compliance

Non-compliance with this AML policy, whether intentional or unintentional, may lead to internal disciplinary measures and/or legal and regulatory consequences. These may include:

- Internal disciplinary actions, including formal warnings, suspension, or termination of employment or business relationships;
- Regulatory sanctions, including revocation of the Company's license or financial penalties imposed by the GCB or other competent authorities;
- Legal penalties, as defined under the NOIS and NORUT, including:

- Fines for failure to comply with reporting obligations;
- Fines per day for ongoing non-compliance;
- Criminal prosecution for serious violations, and/or administrative fines for intentional offenses;

10.2 Reporting and Enforcement

The MLRO is responsible for ensuring compliance oversight across the Company. Any employee who becomes aware of a potential breach of this policy must report it directly to the MLRO without delay.

The Company will cooperate fully with the FIU Curaçao, GCB, and other competent authorities in any investigation or enforcement action and will maintain records of all such interactions.

11. Reporting of Unusual Transactions and Suspicious Activity

Although the Company does not maintain direct relationships with end users or players, it has a legal obligation under the National Ordinance on the Reporting of Unusual Transactions (NORUT) and AML/CTF supervisory regulations to monitor and report any unusual or suspicious activity observed in its B2B operations.

All employees must remain alert to indicators of potential money laundering, terrorist financing, or proliferation financing through the Company's business relationships or service channels.

11.1 Types of Reportable Transactions

In the B2B context, examples of unusual or suspicious activity may include, but are not limited to:

- A B2B client conducting large or frequent payments that are inconsistent with the expected volume or declared activity.
- Clients with sudden changes in jurisdiction or ownership structure, especially if linked to high-risk or non-transparent locations.
- Failure to provide updated corporate, licensing, or UBO information despite repeated requests.
- Transactions routed through complex or obscure third-party structures, which appear to lack economic rationale.
- Adverse media or intelligence on a client, suggesting involvement in illegal or sanctioned activities.

11.2 Internal Escalation and Reporting to FIU

Any employee who identifies a transaction or business relationship that may qualify as unusual or suspicious must report it immediately to the Money Laundering Reporting Officer (MLRO). The MLRO is responsible for assessing the report and determining whether there is sufficient basis to submit a Unusual Transaction Report (UTR).

UTRs must be submitted without delay via the official FIU portal and must include all relevant supporting documentation and reasoning for suspicion.

11.3 Record-Keeping

The Company shall maintain a secure internal log of all internal reports submitted to the MLRO, along with a record of UTRs submitted to the FIU. These records must be retained for at least five years, as required by Curaçao law.

11.4 Confidentiality and Non-Tipping Off

All reports and investigations related to suspicious activity are strictly confidential. Employees are strictly prohibited from disclosing to any client or external party that a report has been made or that an investigation is underway.

12. Record-Keeping

The Company maintains all records relevant to its anti-money laundering and counter-terrorist financing obligations in accordance with the applicable laws and regulations.

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

- Customer Due Diligence (CDD) documentation, including identification forms, company documents, beneficial ownership verification, and Enhanced Due Diligence materials (if applicable).
- Business correspondence and communication logs related to onboarding, monitoring, and AML-related matters.
- Transaction records, including invoices, contracts, and payment documentation, sufficient to reconstruct the nature and purpose of any business activity or transaction.
- Internal reports of unusual or suspicious activity, including documentation of decisions not to file a report.
- Records of reports submitted to the FIU Curaçao, including confirmation of receipt and any follow-up correspondence.
- Training records, demonstrating employee participation in AML/CTF education and updates.

All records are stored securely, in either digital or physical form, and are accessible only to authorised personnel. The Company ensures that records can be promptly retrieved and submitted upon lawful request.

13. Employee Training and Awareness

The Company recognises that an effective AML/CTF compliance framework requires continuous employee training and awareness. All relevant personnel must possess a clear understanding of their responsibilities under applicable AML/CTF regulations and internal procedures.

13.1 Training Program

The Company has implemented an internal AML/CTF training program designed to ensure that employees:

- Understand the legal obligations under AML legislation;
- Are aware of money laundering and terrorist financing risks relevant to B2B operations;
- Can identify indicators of suspicious or unusual activity specific to the Company's business model;
- Know how and when to escalate suspicious behaviour or transactions to the Money Laundering Reporting Officer (MLRO);
- Are familiar with the Company's internal procedures for due diligence, client onboarding, ongoing monitoring, and reporting obligations.

13.2 Frequency and Scope

Training is provided to new staff during onboarding and must be completed before any AML-sensitive tasks are performed. Refresher training is conducted at least annually and may be updated more frequently to reflect:

- Changes in legislation or regulatory guidance;
- Revisions to internal policies and procedures;
- Emerging typologies and red flags in the industry;
- Feedback or findings from reviews.

13.3 Training Records

The Company maintains documented evidence of all AML/CTF training activities, including:

- Names of participants;
- Date and duration of training;
- Content covered;
- Results of knowledge assessments

Records are retained for a minimum of five (5) years.

Approved:

Xecutive Corporate Management B.V.

Date: 25.05.2025