

**Anti-Money Laundering and Counter-Terrorism Financing Policy  
(AML/CFT Policy)**

**Oxilium N.V.  
Company Number: 165075  
Dr. M. J. Hugenholtzweg 25,  
Willemstad, Curaçao**

Last Updated: 15<sup>th</sup> December 2025

1. Policy Statement
2. Purpose
3. Legal Basis
4. Definitions
5. Policy Implementation
  - 5.1 Business Risk Assessment
  - 5.2 Customer Risk Assessment
  - 5.3 Customer Acceptance Policy
  - 5.4 Customer Due Diligence
  - 5.5 Ongoing Monitoring
  - (A) Sanctions & Targeted Financial Sanctions (TFS)
  - (B) Cryptocurrency & Emerging Technology Controls
  - 5.6 Reliance on Third Parties to Perform Customer Due Diligence
  - 5.7 Reporting of Unusual Transactions
  - 5.8 Anti-Money Laundering Compliance Program
6. Compliance and Consequences of Non-Compliance
7. Related Information
8. Contact Information
9. Policy History
10. Policy URL (if applicable)

## 1. Policy Statement

Oxilium N.V. (“the Company”) is fully committed to the prevention, detection, and reporting of money laundering, terrorist financing, and proliferation financing in all aspects of its operations. The Company adopts a **zero-tolerance policy** toward any illicit financial activity and is dedicated to maintaining the highest standards of integrity, transparency, and compliance with applicable laws and regulations of Curaçao.

This Policy is established in accordance with the *National Ordinance on the Identification of Natural Persons and Legal Entities (N.O.I.S.)*, the *National Ordinance on the Reporting of Unusual Transactions (N.O.R.U.T.)*, the *Sanctions National Ordinance*, the *Kingdom Sanction Act*, and the *Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025)* issued by the **Curaçao Gaming Authority (CGA)**.

The Company recognizes its responsibility to ensure that its gaming platforms, payment systems, and associated services are not misused by criminals or terrorist organizations. To this end, Oxilium N.V. has implemented comprehensive internal procedures, governance measures, and technological safeguards that meet or exceed the requirements of Curaçao law and the recommendations of the **Financial Action Task Force (FATF)**.

Senior Management and the Board of Directors have endorsed this Policy as part of the Company’s governance framework. They hold ultimate responsibility for ensuring that all employees, agents, and third-party partners act in full compliance with AML/CFT/CPF requirements and the principles of ethical conduct.

All Company personnel must:

- Comply with the letter and spirit of this Policy;
- Participate in AML/CFT/CPF training and awareness programs;
- Report any suspicious or unusual activity immediately through designated internal channels; and
- Cooperate fully with the Compliance Officer and relevant regulatory or law enforcement authorities.

Failure to comply with this Policy may lead to disciplinary action, termination of employment or contract, and potential legal consequences under Curaçao law.

## 2. Purpose

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing Policy (“the Policy”) is to define the principles, framework, and responsibilities that guide Oxilium N.V. (“the Company”) in the prevention, detection, and reporting of activities related to money laundering, terrorist financing, and proliferation financing.

This Policy aims to:

- Ensure full compliance with the National Ordinance on the Identification of Natural Persons and Legal Entities (N.O.I.S.), the National Ordinance on the Reporting of Unusual Transactions (N.O.R.U.T.), and the Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025);
- Safeguard the Company and its stakeholders from reputational, financial, and regulatory risk;
- Establish clear internal responsibilities for compliance across all business units and functions;
- Define and maintain a risk-based approach (RBA) to the identification and management of AML/CFT/CPF risks;
- Promote a strong compliance culture within the Company; and

- Ensure effective cooperation with competent authorities, including the Curaçao Gaming Authority (CGA), the Financial Intelligence Unit (FIU Curaçao), and other relevant agencies.

This Policy forms an integral part of the Company's overall compliance framework and must be read together with the Customer Due Diligence Procedures, Transaction Monitoring Guidelines, Employee Screening Policy, and other relevant internal documents.

All employees, management, and partners are expected to act in accordance with the principles set forth herein and to exercise sound judgment in situations that may pose potential AML/CFT/CPF risks to the Company or the jurisdiction of Curaçao.

### 3. Legal Basis

This Policy is established pursuant to the applicable laws and regulations of Curaçao that govern the prevention of money laundering, terrorist financing, and proliferation financing. The Company's Anti-Money Laundering and Counter-Terrorist Financing framework is designed to ensure full compliance with the following legal instruments:

1. **National Ordinance on the Identification of Natural Persons and Legal Entities (N.O.I.S.)** - establishing requirements for customer identification, verification, and record-keeping obligations.
2. **National Ordinance on the Reporting of Unusual Transactions (N.O.R.U.T.)** - prescribing obligations to identify and report unusual transactions to the Financial Intelligence Unit (FIU Curaçao).
3. **Sanctions National Ordinance and Kingdom Sanction Act** - mandating compliance with international sanctions and the freezing of assets related to designated individuals, organizations, or countries.
4. **Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025)** - issued by the Curaçao Gaming Authority (CGA), outlining detailed compliance and reporting obligations for licensed gaming operators.
5. **National Ordinance on Offshore Games of Hazard (NOOGH)** and related regulations - establishing the licensing and supervisory framework for online gaming operators in Curaçao.
6. **Applicable international standards and recommendations of the Financial Action Task Force (FATF)** - providing globally recognized principles for AML/CFT/CPF risk management.

This Policy also adheres to all applicable Guidance Notes, Circulars, Technical Standards and supervisory communications issued by the Curaçao Gaming Authority (CGA), including those relating to customer onboarding, transaction monitoring, cryptocurrency risk management and reporting obligations, as amended from time to time, including the CGA 'Crypto policy guideline for online gaming operators' (December 2025), where applicable.

The Company acknowledges that compliance with these laws is both a **legal requirement** and a **moral obligation** that supports the integrity of the financial and gaming sectors of Curaçao.

This Policy, together with the Company's internal AML procedures, training programs, and risk-based controls, ensures adherence to all relevant statutory obligations. It shall be reviewed and updated periodically to reflect changes in Curaçao's legal and regulatory environment, as well as evolving international standards and industry best practices.

### 4. Definitions

For the purposes of this Policy, the following definitions apply:

- **AML/CFT/CPF:** Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of the Proliferation of Weapons of Mass Destruction.

- **The Company / Oxilium N.V.:** Refers to Oxilium N.V., a company incorporated under the laws of Curaçao, holder of Gaming Licence No. OGL/2024/1601/0909, regulated by the Curaçao Gaming Authority.
- **CGA:** The *Curaçao Gaming Authority*, the designated supervisory authority responsible for overseeing compliance with AML/CFT/CPF obligations by licensed gaming operators under the LOK regime.
- **FIU Curaçao:** The *Financial Intelligence Unit of Curaçao* (“Meldpunt Ongebruikelijke Transacties”), the competent authority responsible for receiving, analyzing, and disseminating reports of unusual transactions.
- **Money Laundering:** The process by which criminals conceal the origins of illegally obtained funds, making them appear legitimate. It includes placement, layering, and integration of proceeds of crime.
- **Terrorist Financing:** The provision or collection of funds, by any means, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, for terrorist purposes.
- **Proliferation Financing:** The provision of funds or financial services used for the manufacture, acquisition, possession, transport, or transfer of nuclear, chemical, or biological weapons and their means of delivery, contrary to international law.
- **Customer:** Any natural or legal person who applies for, uses, or maintains an account, gaming service, or business relationship with the Company, whether directly or through an intermediary.
- **Business Relationship:** A relationship established between the Company and a Customer that is expected, at the time of establishment, to have an element of duration.
- **Beneficial Owner (UBO):** The natural person(s) who ultimately owns or controls the Customer and/or the natural person on whose behalf a transaction or activity is conducted, as defined in the N.O.I.S.
- **Customer Due Diligence (CDD):** The process of identifying and verifying the identity of a Customer, beneficial owner, and the purpose and intended nature of the business relationship, in accordance with Curaçao law.
- **Enhanced Due Diligence (EDD):** Additional and more detailed verification procedures applied to Customers or transactions that present a higher risk of money laundering, terrorist financing, or proliferation financing.
- **Suspicious / Unusual Transaction:** A transaction that, based on its characteristics, frequency, size, or nature, deviates from normal patterns and gives rise to suspicion that it may be connected with money laundering or terrorist financing.
- **Sanctions List:** Any list issued or adopted by the United Nations, the European Union, the Kingdom of the Netherlands, or the Curaçao authorities, identifying individuals or entities subject to targeted financial sanctions.
- **Compliance Officer (MLRO):** The designated officer responsible for ensuring the Company’s compliance with all AML/CFT/CPF obligations, maintaining liaison with CGA and FIU Curaçao, and overseeing implementation of this Policy.
- **Risk-Based Approach (RBA):** A methodology whereby the Company identifies, assesses, and mitigates risks associated with money laundering and terrorist financing in proportion to the level of risk identified.
- **Politically Exposed Person (PEP):** An individual who is or has been entrusted with a prominent public function, as well as their immediate family members and close associates, in accordance with FATF and N.O.I.S. definitions.
- **Third Party / Service Provider:** Any external entity performing part of the Company’s AML/CFT/CPF obligations, such as KYC verification providers, payment processors, or agents, under written agreement and supervision.

## 5. Policy Implementation

The implementation of this Policy ensures that Oxilium N.V. maintains a comprehensive and effective system to prevent and detect money laundering, terrorist financing, and proliferation financing.

All measures described in this section are applied proportionately, based on the Company's risk-based approach (RBA) and consistent with Curaçao's legal and regulatory framework.

Senior Management, the Board of Directors, and all employees share collective responsibility for the implementation of this Policy. The Compliance Officer (MLRO) has operational responsibility for overseeing compliance, monitoring implementation, and reporting to relevant authorities.

The Company's AML/CFT/CPF framework is based on eight interrelated components, as set out below:

- 5.1 Business Risk Assessment (BRA)
- 5.2 Customer Risk Assessment (CRA)
- 5.3 Customer Acceptance Policy (CAP)
- 5.4 Customer Due Diligence (CDD)
- 5.5 Ongoing Monitoring
- 5.6 Reliance on Third Parties to Perform CDD
- 5.7 Reporting of Unusual Transactions
- 5.8 AML Compliance Program

Each of these components is mandatory and must be applied consistently across all operations, products, and jurisdictions where the Company conducts business.

#### **5.1 Business Risk Assessment (BRA)**

The Company maintains a documented Business Risk Assessment (BRA) to identify and evaluate the risks of money laundering, terrorist financing, and proliferation financing to which it is exposed. The BRA is reviewed and updated at least annually, or earlier if there are significant changes to the Company's business model, customer base, jurisdictions of operation, or delivery channels.

The BRA covers, at minimum, the following areas:

- The nature, scale, and complexity of the Company's operations;
- The types of products and services offered (including gaming, payment processing, and digital assets, if applicable);
- The categories of customers and counterparties engaged;
- The jurisdictions in which the Company operates or provides access;
- The channels through which services are offered (e.g., online platforms, affiliates, agents); and
- Emerging typologies and threats identified by the CGA, FIU Curaçao, or FATF.

The results of the BRA are used to:

- Inform the design of internal controls and risk mitigation strategies;
- Determine the level of resources allocated to compliance and monitoring;
- Support the Customer Risk Assessment (CRA) and Customer Acceptance Policy (CAP); and
- Report material findings to Senior Management and the CGA upon request.

The BRA shall be approved by the Board of Directors and maintained as part of the Company's official compliance records.

All relevant staff must be familiar with the identified risks and understand their role in mitigating them.

#### **5.2 Customer Risk Assessment (CRA)**

Oxilium N.V. (“the Company”) applies a **Customer Risk Assessment (CRA)** process to evaluate the level of AML/CFT/CPF risk associated with each customer before establishing a business relationship or executing transactions.

The CRA forms part of the Company’s overall **Risk-Based Approach (RBA)** and ensures that customers presenting higher risks are subject to enhanced due diligence (EDD) and stricter monitoring procedures.

### **5.2.1 Risk Categories**

Each customer is assigned a risk rating based on an assessment of the following four primary categories:

1. **Customer Profile Risk** - nature of the customer (individual or corporate), source of funds, source of wealth, occupation or business activity, and ownership or control structure (including UBO analysis).
2. **Geographical Risk** - jurisdictions of residence, incorporation, or activity; exposure to high-risk or non-cooperative countries identified by FATF, EU, or CGA lists.
3. **Product / Service Risk** - type of product or gaming service used, payment channels (credit card, crypto, wire, etc.), transaction volumes, and patterns of play.
4. **Delivery Channel Risk** - method of customer interaction (remote onboarding, affiliate-based acquisition, agent channel), degree of non-face-to-face verification, and technology risks.

### **5.2.2 Risk Scoring and Rating**

The Company maintains an internal risk-scoring model that categorizes customers as **Low**, **Medium**, or **High Risk**.

Key parameters are defined in the Company’s internal *Customer Risk Assessment Matrix*, reviewed annually by the Compliance Officer.

Examples:

- **Low Risk:** Long-term customers with verified identity, clear source of funds, operating in low-risk jurisdictions.
- **Medium Risk:** Customers using multiple payment methods, moderate transaction volumes, or from jurisdictions with enhanced monitoring requirements.
- **High Risk:** Politically Exposed Persons (PEPs), customers from FATF high-risk countries, or those whose activities involve anonymity-enhancing technologies or complex ownership chains.

### **5.2.3 Risk Mitigation and Review**

- All **High-Risk Customers** are subject to **Enhanced Due Diligence (EDD)**, requiring senior-management approval prior to onboarding.
- The CRA must be **documented, justified, and retained** as part of the customer’s compliance file for at least five years after termination of the relationship.
- Risk ratings are reviewed periodically or when a trigger event occurs (e.g., unusual transaction, change in ownership, negative media, or sanction alert).
- The CRA informs the **Ongoing Monitoring** program (Section 5.5) and supports decision-making on whether to maintain or terminate the relationship.

### **5.2.4 Tools and Data Sources**

The Company utilizes both internal monitoring systems and reputable third-party tools (e.g., KYC, PEP, Sanctions and Adverse Media Screening providers) to ensure reliable and up-to-date data for the CRA process.

The Compliance Officer (MLRO) is responsible for reviewing the effectiveness of these tools and documenting any updates in the annual Compliance Report.

### 5.3 Customer Acceptance Policy (CAP)

Oxilium N.V. (“the Company”) maintains a **Customer Acceptance Policy (CAP)** that defines the principles and criteria under which it will establish and maintain business relationships with customers. The objective of this policy is to ensure that the Company engages only with customers whose identities, activities, and sources of funds can be reasonably verified and justified in accordance with Curaçao’s AML/CFT/CPF regulations.

The Company shall not enter into or maintain a business relationship where it cannot apply adequate **Customer Due Diligence (CDD)** measures or where the customer fails or refuses to provide required information or documentation.

#### 5.3.1 General Principles

The following general principles guide the Company’s Customer Acceptance Policy:

1. **No Anonymous or Fictitious Accounts.**

The Company prohibits the opening or maintenance of anonymous or fictitious player accounts. All accounts must be registered under the verified true identity of the customer.

2. **Verification Prior to Relationship Establishment.**

The Company shall complete the identification and verification of a customer before activating any gaming account, processing deposits, or permitting participation in any wagering activity.

3. **Risk-Based Decision to Onboard.**

Customer onboarding decisions are based on the outcomes of the **Customer Risk Assessment (CRA)**. High-risk customers may be accepted only after **Enhanced Due Diligence (EDD)** and **senior management approval**.

4. **Prohibition of Relationships with Certain Categories.**

The Company shall not accept or maintain relationships with:

- Customers located in or associated with **restricted or sanctioned jurisdictions** as defined in the CGA’s Restricted Territories List (Specifically, the Company must not onboard, service, or allow gameplay from customers located in, or associated with, the following jurisdictions: Aruba, Australia, Austria, Bonaire, Curaçao, Saba, Sint Eustatius, The Netherlands, Belgium, France, Spain, Germany, Greece, Czech Republic, Lithuania, and the United States of America. This Restricted Territories List must be reviewed quarterly and updated immediately upon receipt of any revisions or notices issued by the Curaçao Gaming Authority.);
- **Shell companies** or legal entities with no legitimate commercial purpose;
- Customers using **anonymizing technologies** (e.g., VPNs, TOR networks) to conceal their true location or identity;
- Customers who appear on **any relevant sanctions or watch lists**, including UN, EU, OFAC, or Kingdom of the Netherlands lists;
- Customers involved in industries considered high-risk under FATF or CGA guidance (e.g., unregulated crypto exchanges, arms trade, or politically exposed activities without sufficient justification).

5. **Acceptance Criteria for Corporate Customers.**

When dealing with corporate or institutional customers, the Company must identify and verify:

- The legal existence and status of the entity;
- The identity of directors, authorized signatories, and ultimate beneficial owners (UBOs);
- The nature and purpose of the entity’s business and its expected transactional profile.

6. **Customer Screening Prior to Acceptance.**

All new customers shall be screened against sanctions, PEP, and adverse media databases before acceptance. Screening results must be documented and reviewed by the Compliance Officer.

### **5.3.2 Approval and Escalation**

- **Low and Medium-Risk Customers** may be approved by the Customer Verification Team, in line with defined onboarding procedures.
- **High-Risk Customers** require written approval from the **Compliance Officer (MLRO)** or a member of **Senior Management** before account activation.
- Any exception to the CAP must be documented, justified, and approved at a senior level, with corresponding records retained.

### **5.3.3 Refusal and Termination**

The Company reserves the right to **refuse onboarding** or **terminate an existing relationship** if:

- Identification or verification documents cannot be obtained or validated;
- The customer provides false, incomplete, or misleading information;
- There is reasonable suspicion of money laundering, terrorist financing, or other criminal conduct;
- The customer engages in activities that expose the Company to reputational or regulatory risk.

All refusals and terminations related to AML/CFT concerns must be recorded in the Company's **Rejection & Termination Register**, which shall be accessible to the Compliance Officer and CGA upon request.

## **5.4 Customer Due Diligence (CDD)**

Oxilium N.V. ("the Company") shall perform **Customer Due Diligence (CDD)** on all new and existing customers, beneficial owners, and relevant third parties in accordance with the *National Ordinance on the Identification of Natural Persons and Legal Entities (N.O.I.S.)* and the *Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025)*.

The objective of CDD is to establish and verify the true identity of customers and beneficial owners, understand the purpose and intended nature of the relationship, and determine the legitimacy of their funds and activities.

### **5.4.1 Timing of CDD**

- CDD must be completed **before** a customer is permitted to open an account, deposit funds, or engage in gaming activity.
- No exceptions shall be granted for high-risk customers or transactions.
- Where verification cannot be completed prior to commencement for technical reasons, it must be finalized **as soon as reasonably practicable** and always before any withdrawal or payout.
- Ongoing CDD must be performed on existing customers when:
  - there is a material change in their profile or risk rating;
  - the Company detects unusual activity patterns; or
  - new information emerges that may affect risk classification.

### **5.4.2 Identification and Verification Requirements**

The Company shall collect and verify at least the following information:

**For Individual Customers:**

- Full name, date of birth, and nationality;
- Residential address and contact information;
- Valid government-issued photo identification (passport or national ID);
- Source of funds and, where relevant, source of wealth;
- Occupation or employment information.

**For Corporate Customers:**

- Full legal name, registration number, and date of incorporation;
- Registered office address and principal place of business;
- Memorandum and Articles of Association (or equivalent);
- Identity of directors, authorized signatories, and **Ultimate Beneficial Owners (UBOs)** holding 25% or more ownership or control;
- Nature and purpose of the business relationship;
- Source of funds and expected transaction volumes.

All documents must be **current, authentic, and independently verified** via reliable sources or third-party verification systems (KYC providers).

#### ***5.4.3 Enhanced Due Diligence (EDD)***

The Company applies **Enhanced Due Diligence (EDD)** to customers classified as **high risk** under the Customer Risk Assessment (Section 5.2).

EDD measures include, but are not limited to:

- Obtaining senior management approval prior to onboarding;
- Collecting additional documentation regarding source of funds and source of wealth;
- Conducting enhanced adverse media and sanctions screening;
- Performing independent background checks or open-source intelligence (OSINT) reviews;
- Implementing heightened transaction monitoring rules and manual reviews.

**Politically Exposed Persons (PEPs)** and their close associates shall always be treated as high-risk customers and subject to EDD procedures.

#### ***5.4.4 Simplified Due Diligence (SDD)***

Where the risk is assessed as **low**, and only after documented justification by the Compliance Officer, the Company may apply Simplified Due Diligence (SDD).

However, the following conditions must be met:

- No indicators of suspicious or unusual activity exist;
- The customer is resident in a jurisdiction with equivalent AML/CFT standards; and
- The customer is not a PEP or linked to any high-risk industry or jurisdiction.

#### ***5.4.5 Ongoing CDD and Recordkeeping***

The Company must ensure that all customer information remains current and accurate. Periodic reviews of CDD files shall be conducted based on risk level as follows:

- **Low Risk:** Every 3 years
- **Medium Risk:** Every 2 years
- **High Risk:** Annually or upon trigger event

All CDD records must be retained for at least **five (5) years** after the termination of the relationship and must be readily available to the CGA and FIU Curaçao upon request.

## 5.5 Ongoing Monitoring

Oxilium N.V. (“the Company”) maintains continuous monitoring of all customer accounts, transactions, and behavioral patterns to detect, prevent, and report any suspicious or unusual activity that could indicate money laundering, terrorist financing, or proliferation financing.

Ongoing monitoring ensures that customer activity is consistent with the Company’s knowledge of the customer, their risk profile, source of funds, and expected level of gaming or transactional behavior.

### 5.5.1 Monitoring Objectives

The objectives of ongoing monitoring are to:

- Identify deviations from normal transactional behavior;
- Detect complex, unusually large, or inconsistent transactions;
- Recognize patterns or activity inconsistent with the stated purpose of the relationship;
- Ensure that customer information and risk classification remain up to date; and
- Facilitate timely reporting of unusual transactions to the FIU Curaçao.

### 5.5.2 Monitoring Methods

The Company employs both **automated and manual monitoring systems** designed to flag potentially suspicious transactions or patterns.

These systems are configured to detect:

- Rapid deposits and withdrawals without clear gaming activity;
- Use of multiple payment methods or accounts by a single customer;
- Activity inconsistent with the customer’s declared source of funds;
- Transactions involving high-risk jurisdictions or intermediaries;
- Round-sum transactions or structured deposits to avoid thresholds;
- Attempts to bypass KYC controls or self-exclusion mechanisms.

All alerts generated by monitoring systems are subject to review by the **Compliance Team**, with escalation to the **Compliance Officer (MLRO)** when warranted.

### 5.5.3 Frequency and Intensity

The frequency and intensity of monitoring correspond to the customer’s risk level.

- **High-Risk Customers** - continuous, real-time monitoring with manual review of flagged transactions;
- **Medium-Risk Customers** - periodic automated monitoring with sampling by Compliance;
- **Low-Risk Customers** - ongoing automated monitoring with periodic exception review.

Enhanced manual monitoring is also performed for transactions exceeding predefined financial thresholds or involving cryptocurrency or other alternative payment methods.

### 5.5.4 Periodic Review and Updating

Customer information must be updated on a periodic basis as defined in Section 5.4.5. If a customer’s behavior, source of funds, or transaction pattern materially changes, the **Customer Risk Assessment (CRA)** shall be re-evaluated, and appropriate measures (including EDD) applied. Any material findings arising from ongoing monitoring are documented in the **Monitoring & Review Log**, which is maintained by the Compliance Department and subject to Board oversight.

### 5.5.5 Escalation and Reporting

Where monitoring identifies suspicious or unexplained activity.

1. The alert is reviewed by the Compliance Officer.
2. If suspicion is confirmed, an **Unusual Transaction Report (UTR)** is filed promptly with **FIU Curaçao**, in accordance with N.O.R.U.T. requirements.
3. Where necessary, relevant accounts may be **suspended or frozen** pending further review.
4. All decisions and actions are recorded and maintained for audit purposes.

### 5.5. (A) Sanctions & Targeted Financial Sanctions (TFS)

The Company screens all customers and transactions against applicable UN, EU, Kingdom of the Netherlands and Curaçao sanctions lists. Where a match is identified, the Company shall freeze the related funds or assets without delay and without prior notice, refrain from making funds or economic resources available to the designated person or entity, and promptly notify the MLRO. The MLRO shall escalate to the relevant competent authority and ensure records are maintained. Tipping-off is strictly prohibited.

### 5.5 (B) Cryptocurrency & Emerging Technology Controls

Cryptocurrency transactions are treated as high-risk. Where the Company accepts or processes cryptocurrency payments, the Company applies enhanced controls proportionate to risk, including (as applicable): blockchain analytics, wallet screening, exposure checks to sanctioned entities, mixers/tumblers and darknet sources, transaction tracing, asset-specific limits and velocity controls, and enhanced monitoring thresholds and reporting triggers.

Crypto-related controls are implemented in accordance with the Company's Crypto Asset Policy and any applicable CGA guidance and circulars. Where crypto functionality is not enabled, these controls apply on a readiness basis and are activated prior to launching any crypto payment method.

Where crypto is enabled, withdrawals are processed to the same wallet from which the deposit was received and in the same crypto-asset as the deposit, subject to applicable compliance checks. Player-to-player transfers are prohibited. The Company uses only entity-owned wallets and routes crypto flows via regulated/registered VASPs/exchanges subject to due diligence and ongoing monitoring. The Company does not provide exchange services.

Where applicable, the Company holds operational crypto wallets with regulated/registered exchanges/VASPs (no self-custody by individuals), subject to segregation and access controls.

### 5.6 Reliance on Third Parties to Perform Customer Due Diligence

Oxilium N.V. ("the Company") may rely on duly regulated and reputable third parties to perform certain elements of the Customer Due Diligence (CDD) process, provided that such reliance fully complies with Curaçao AML/CFT/CPF regulations and that the Company retains ultimate responsibility for compliance.

Third parties may include:

- Independent **KYC / identity verification providers**;
- **Payment service providers (PSPs)** and financial institutions regulated within the European Union or equivalent jurisdictions;

- **Affiliates or agents** performing limited customer onboarding functions under contractual agreement; or
- **Corporate service providers** conducting verification of legal entities or beneficial owners.

#### **5.6.1 Conditions for Reliance**

Reliance on third parties is permissible only when **all of the following conditions** are satisfied:

1. The third party is subject to AML/CFT/CPF laws and supervision in a jurisdiction that is compliant with **FATF standards** or otherwise deemed equivalent by the CGA.
2. A **written agreement** is in place clearly outlining:
  - the scope of CDD activities to be performed,
  - data protection and confidentiality obligations,
  - record-keeping and audit access rights,
  - reporting timelines and escalation procedures.
3. The Company has obtained **immediate access** to all CDD documentation, verification data, and risk assessments collected by the third party.
4. The Company has conducted due diligence on the third party to confirm its regulatory status, competence, and reliability prior to reliance.
5. The **ultimate responsibility** for compliance with AML/CFT/CPF obligations remains with the Company at all times.

#### **5.6.2 Supervision and Oversight**

- The Compliance Officer (MLRO) shall maintain a **Third-Party Reliance Register** containing:
  - details of each third party relied upon,
  - copies of the contractual agreements,
  - the results of annual due-diligence reviews, and
  - confirmation of FATF-equivalent jurisdictional status.
- The Compliance Officer shall periodically test and evaluate the adequacy of third-party CDD processes and documentation.
- Any deficiencies or breaches must be reported to Senior Management and, where necessary, to the **Curaçao Gaming Authority (CGA)**.

#### **5.6.3 Termination of Reliance**

If a third party:

- fails to provide requested verification data in a timely manner,
- loses its regulated status,
- is found to be non-compliant with AML/CFT obligations, or
- operates from a non-equivalent jurisdiction,

the Company shall immediately **cease reliance** and perform its own full CDD on the affected customers.

### **5.7 Reporting of Unusual Transactions**

Oxilium N.V. (“the Company”) shall promptly identify, review, and report any transaction or attempted transaction that may be considered **unusual or suspicious** under Curaçao law. The obligation to report arises under the *National Ordinance on the Reporting of Unusual Transactions*

(N.O.R.U.T.) and the *Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025)*.

#### ***5.7.1 Identification and Internal Reporting***

All employees and contractors of the Company are required to remain vigilant for indicators of suspicious or unusual activity. When such activity is identified, the employee must immediately file an **Internal Suspicion Report (ISR)** to the **Compliance Officer (MLRO)** using the designated reporting form or secure internal channel.

Examples of indicators include (but are not limited to):

- Transactions inconsistent with a customer's known profile or source of funds;
- Rapid deposits and withdrawals without clear gaming activity;
- Use of multiple accounts or third-party payment methods;
- Attempts to circumvent CDD or transaction limits;
- Repeated declines or failed verifications associated with structured behavior;
- Links to high-risk or sanctioned jurisdictions.

#### ***5.7.2 MLRO Review and External Reporting***

The Compliance Officer (MLRO) is responsible for evaluating all Internal Suspicion Reports to determine whether an external report to **FIU Curaçao** is warranted. Where suspicion cannot be reasonably eliminated, the MLRO must file an **Unusual Transaction Report (UTR)** with FIU Curaçao **without delay**, using the official FIU reporting portal and templates.

Key obligations:

- Reporting must occur **as soon as possible** after suspicion arises and **before** tipping-off the customer;
- All supporting documentation (KYC, transaction logs, correspondence) must accompany the UTR submission;
- The MLRO must maintain full confidentiality regarding the identity of the reporting employee.

#### ***5.7.3 Tipping-Off Prohibition***

Employees and management are strictly prohibited from **informing or alerting** any customer, third party, or external entity that a UTR has been filed or that their activities are under review. Any breach of this prohibition constitutes a serious disciplinary offence and may lead to termination of employment and potential criminal liability under Curaçao law.

#### ***5.7.4 Recordkeeping and Audit Trail***

The Company shall maintain a **UTR Register** that includes:

- the date of detection,
- internal reference number,
- nature of the suspicion,
- actions taken, and
- confirmation of UTR submission (where applicable).

All records, reports, and supporting documentation related to UTRs must be retained for at least **five (5) years** from the date of filing and made available to the **Curaçao Gaming Authority (CGA)** or **FIU Curaçao** upon request.

#### ***5.7.5 Cooperation with Authorities***

The Company shall fully cooperate with the FIU Curaçao, CGA, and any other competent law enforcement agencies in the investigation of reported or suspected money laundering or terrorist financing cases. All requests for additional information from the FIU or CGA must be responded to **promptly and accurately**.

The Compliance Officer is authorized to liaise directly with FIU Curaçao on behalf of the Company and shall ensure that all communications are securely documented.

#### **5.8 Anti-Money Laundering Compliance Program**

Oxilium N.V. (“the Company”) has implemented a comprehensive **Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing Compliance Program** (“the Program”) to ensure effective and ongoing compliance with Curaçao’s AML/CFT/CPF legal framework and regulatory requirements issued by the **Curaçao Gaming Authority (CGA)**.

The Program integrates governance, control, training, monitoring, and audit mechanisms designed to prevent, detect, and respond to any activity that may involve money laundering, terrorist financing, or proliferation financing.

##### ***5.8.1 Appointment of Compliance Officer (MLRO)***

The Company has appointed a qualified and experienced **Compliance Officer**, also referred to as the **Money Laundering Reporting Officer (MLRO)**, approved by the Board of Directors.

The Compliance Officer is responsible for:

- Overseeing the implementation and maintenance of this Policy;
- Acting as the primary point of contact with the CGA and FIU Curaçao;
- Reviewing and reporting all suspicious or unusual activities;
- Maintaining the UTR Register and compliance documentation;
- Ensuring timely reporting and regulatory notifications;
- Coordinating staff training and awareness programs;
- Submitting periodic AML/CFT reports to Senior Management and the CGA.

The Compliance Officer must operate with **independence, authority, and direct access** to Senior Management and the Board. Any conflicts of interest shall be declared and mitigated.

##### ***5.8.2 Training and Awareness***

The Company conducts regular, documented AML/CFT/CPF training for all employees, contractors, and relevant third parties. Training programs are designed to:

- Educate staff on Curaçao AML/CFT/CPF laws and internal procedures;
- Identify red flags and typologies relevant to gaming and payments;
- Reinforce reporting obligations and the prohibition of tipping-off;
- Explain procedures for internal escalation and recordkeeping;
- Address updates in legislation, sanctions regimes, and regulatory expectations.

#### **Frequency of training:**

- **New employees:** within one (1) month of onboarding;

- **Existing employees:** at least once annually;
- **Senior management and MLRO:** advanced training annually or upon regulatory updates.

Attendance and comprehension are documented through sign-off sheets or electronic logs, maintained for **five (5) years**.

### ***5.8.3 Independent Audit Function***

The Company maintains an **independent audit function** to periodically test the effectiveness of the AML/CFT/CPF Program.

The audit shall:

- Be performed at least **once per year** by qualified internal or external professionals independent of the Compliance function;
- Assess the adequacy of internal controls, CDD procedures, transaction monitoring, reporting accuracy, and training programs;
- Produce a written report with findings, recommendations, and timelines for corrective action;
- Audit reports and remediation plans shall be made available to the Curaçao Gaming Authority (CGA) upon request.

### ***5.8.4 Recordkeeping and Documentation***

All documents related to AML/CFT/CPF compliance - including customer identification data, risk assessments, transaction records, reports, training logs, and audit reports - must be maintained securely and be retrievable upon request. Retention periods are as follows:

- **Customer and Transaction Records:** at least 5 years after the end of the business relationship;
- **Training and Audit Records:** at least 5 years after completion.

Records must be stored in a manner that ensures confidentiality, integrity, and readiness for inspection by the **CGA, FIU Curaçao**, or law enforcement authorities.

### ***5.8.5 Program Review and Continuous Improvement***

The AML/CFT/CPF Compliance Program is reviewed at least annually, or sooner if:

- There are changes to Curaçao's AML/CFT/CPF legislation or regulations;
- Internal audits or CGA inspections identify weaknesses;
- New products, technologies, or business models introduce new risks.

The Compliance Officer is responsible for initiating updates and ensuring that all staff are informed and trained on any revisions.

### ***5.8.6 Employee Screening***

The Company maintains a documented employee screening program proportionate to role and risk.

Screening is performed:

- **prior to appointment / onboarding (pre-employment);**
- **at least annually for high-risk roles; and**
- **on an ad-hoc basis upon role change, incident, or credible adverse information.**

**Pre-employment and periodic checks (including identity verification, integrity/red-flag checks and, where permitted by law, criminal record checks for key roles) are required for personnel involved in onboarding, payments, compliance or access to sensitive systems. Screening outcomes are recorded and retained for a minimum of five (5) years.**

High-risk roles include personnel involved in customer onboarding and verification, payments and withdrawals, transaction monitoring, compliance, and system administration with access to sensitive systems or regulated data.

Any adverse findings or red flags are escalated to the Compliance Officer (CO/MLRO) for documented assessment and decision. Outcomes may include enhanced supervision, restriction of duties, suspension, termination, or reporting to the competent authority where required.

## **6. Compliance and Consequences of Non-Compliance**

Oxilium N.V. (“the Company”) is fully committed to complying with all applicable laws, regulations, and regulatory guidance governing Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CFT/CPF) in Curaçao.

Compliance with this Policy and the related procedures is **mandatory** for all employees, officers, contractors, agents, and third-party service providers acting on behalf of the Company. Every individual has a personal responsibility to adhere to the requirements of Curaçao’s AML/CFT/CPF framework and to act with honesty, transparency, and diligence when performing duties related to customer onboarding, payments, or transaction monitoring.

### ***6.1 Management Oversight***

Senior Management and the Board of Directors are ultimately responsible for ensuring that:

- The Company maintains effective internal controls, governance, and reporting mechanisms;
- Adequate resources (human, technical, and financial) are allocated to the Compliance function;
- The Compliance Officer (MLRO) operates independently and has unrestricted access to management and information;
- Regular reviews and reports on AML/CFT/CPF performance are presented and acted upon.

Management shall promote a culture of compliance throughout the organization and ensure that any deficiencies identified by the Compliance Officer, internal audit, or the CGA are addressed promptly.

### ***6.2 Employee Responsibilities***

All employees must:

- Comply with the procedures outlined in this Policy;
- Complete AML/CFT/CPF training and refresher programs as required;
- Immediately report suspicious activity to the Compliance Officer;
- Maintain the confidentiality of all information related to AML/CFT/CPF investigations; and
- Cooperate fully with the Compliance Officer, auditors, and regulatory authorities.

Failure to meet these obligations will be treated as a serious violation of Company policy.

### ***6.3 Disciplinary and Legal Consequences***

Non-compliance with this Policy, Curaçao AML/CFT/CPF legislation, or any related procedure may result in disciplinary action, including:

- Formal warning or reprimand;

- Suspension or termination of employment or contractual relationship;
- Civil penalties or criminal prosecution in accordance with Curaçao law; and
- Reporting of the individual or incident to the relevant regulatory or law-enforcement authority.

The Company reserves the right to take immediate corrective measures where non-compliance may expose it to legal, regulatory, or reputational risk.

#### ***6.4 Continuous Accountability***

Every member of staff must understand that AML/CFT/CPF compliance is a **continuous obligation**, not a one-time event. Ongoing vigilance, timely reporting, and proactive engagement with compliance processes are essential to maintaining the integrity of the Company's operations and its standing as a licensed entity regulated by the **Curaçao Gaming Authority (CGA)**.

#### ***6.5 Escalation and Notification of Material Breaches***

Compliance breaches are escalated in accordance with their severity:

- Level 1 (Minor): procedural deviations with no material impact - handled by line manager and Compliance with documented corrective action.
- Level 2 (Significant): repeated deficiencies, control weaknesses, or staff misconduct affecting AML/CFT controls - escalated to the Compliance Officer (CO/MLRO) and Senior Management with documented remediation timelines.
- Level 3 (Material/Critical): systemic failures, suspected criminal conduct, breaches involving regulated data, customer funds, sanctions/TFS obligations, or control breakdowns - escalated immediately to Senior Management and the Board.

For Level 3 (Material/Critical) breaches, the CO/MLRO will notify the CGA without undue delay and, in any event, no later than five (5) business days after confirming materiality. Where the breach involves sanctions/TFS, customer funds at risk, or suspected criminal conduct, notification will be made as soon as practicable (and where possible within 24-72 hours), subject to any instructions from competent authorities and tipping-off restrictions.

Where required under Curaçao law, CGA regulations, or CGA guidance, the Compliance Officer (CO/MLRO) shall notify the Curaçao Gaming Authority (CGA) without undue delay after confirmation of a material breach and maintain a written incident file, including root cause analysis and remediation actions.

### **7. Related Information**

This Policy must be read in conjunction with the following internal documents, Curaçao legislation, and international standards that collectively form the Company's AML/CFT/CPF framework.

#### ***7.1 Internal Company Policies and Procedures***

- **Customer Due Diligence Procedures Manual** - outlining operational steps for KYC verification, onboarding, and document validation.
- **Transaction Monitoring and Escalation Guidelines** - detailing rules for detecting, flagging, and escalating suspicious transactions.
- **Recordkeeping and Data Retention Policy** - describing how customer and compliance data are securely stored and retained.
- **Employee Screening Policy** - establishing pre-employment and ongoing screening for integrity and fitness.
- **Training and Awareness Program** - defining the scope, frequency, and content of AML/CFT/CPF training.
- **Internal Audit and Testing Procedures** - providing methodology for periodic reviews and compliance assurance.

- **Sanctions Compliance Procedure** - setting forth screening, freezing, and reporting obligations related to UN, EU, and Kingdom of the Netherlands sanctions regimes.

## 7.2 Relevant Curaçao Legislation

- *National Ordinance on the Identification of Natural Persons and Legal Entities (N.O.I.S.)*
- *National Ordinance on the Reporting of Unusual Transactions (N.O.R.U.T.)*
- *Sanctions National Ordinance*
- *Kingdom Sanction Act*
- *Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025)*
- *National Ordinance on Offshore Games of Hazard (NOOGH)*
- All applicable **Guidance Notes and Circulars** issued by the Curaçao Gaming Authority (CGA).

## 7.3 International Standards and Guidance

- *Financial Action Task Force (FATF) 40 Recommendations and Interpretive Notes;*
- *Basel Committee on Banking Supervision - Guidelines on Sound Management of Risks Related to Money Laundering and Financing of Terrorism;*
- *European Union AML Directives (5AMLD and 6AMLD), to the extent applicable;*
- *Egmont Group Principles for Financial Intelligence Units;*
- *Wolfsberg Group Principles on AML/CFT Risk Management.*

These documents and standards form part of the regulatory ecosystem in which the Company operates and are incorporated by reference into this Policy. All updates or amendments to the above instruments shall be reflected in periodic reviews of this Policy, ensuring ongoing compliance with both local and international requirements.

## 8. Contact Information

For any questions, clarifications, or reports related to this Policy or to the Company's Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CFT/CPF) obligations, please contact:

### Money Laundering Reporting Officer (MLRO)

**Name:** Justice Nwankwo

**Position:** Compliance Officer / MLRO

**Company:** Oxilium N.V.

**Business Address:** 1<sup>st</sup> Arch. Kyprianou, Loucaides Building, 3036, Limassol, Cyprus

**Email:** [compliance@bahisbey.com](mailto:compliance@bahisbey.com)

The MLRO serves as the primary point of contact for:

- All internal reports of unusual or suspicious transactions;
- Requests for clarification or additional documentation;
- Cooperation with the **Curaçao Gaming Authority (CGA)** and **FIU Curaçao**;
- Submission of external Unusual Transaction Reports (UTRs) via the designated reporting platform.

If the MLRO is unavailable or a potential conflict of interest exists, communication may be directed to the **Deputy Compliance Officer (DMLRO)** or, where appropriate, directly to the **Board of Directors**.

The MLRO shall ensure that all communications with the **CGA**, **FIU Curaçao**, and other competent authorities are handled promptly, confidentially, and in accordance with the applicable reporting procedures and data protection standards.

## 9. Policy History

This Policy is a controlled document and shall be reviewed, updated, and re-approved at least **annually**, or sooner if:

- There are significant changes in Curaçao's AML/CFT/CPF legislation or regulatory guidance;
- The Company introduces new products, technologies, or markets that alter its risk exposure; or
- The **Compliance Officer / MLRO** identifies operational gaps, emerging risks, or deficiencies in implementation.

All previous versions shall be archived and retained for a minimum of **five (5) years** for regulatory inspection purposes.

This Policy is approved by the Board of Directors and signed off by the Compliance Officer (CO/MLRO).

Signed by Justice Nwankwo in his capacity as Compliance Officer (CO).

### Document Control Table

| Version | Date Approved | Approved By               | Summary of Changes                                                                                                                           | Next Review Date |
|---------|---------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 1.0     | 15/12/2025    | Board of Directors        | Initial issuance of AML/CFT/CPF Policy under Curaçao LOK framework                                                                           | 14/11/2026       |
| 1.1     | 15/12/2025    | Compliance Officer / MLRO | Minor updates to reflect revised CGA Guidance Note 2025                                                                                      | 14/11/2026       |
| 2.0     | 15/12/2025    | Board of Directors        | Comprehensive revision aligned with "Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation (2025)" | 14/11/2026       |

Signature: \_\_\_\_\_

Date: 15/12/2025

Name: Justice Nwankwo

Position: Compliance Officer (CO) / MLRO

All changes to this Policy must be approved by the Board of Directors upon the recommendation of the Compliance Officer / MLRO.

The MLRO shall maintain the official record of document revisions and ensure that the latest approved version is distributed to all relevant staff and made accessible internally.

## 10. Policy URL (if applicable)

This Policy may be made available to relevant stakeholders, including regulatory authorities, auditors, and business partners, through a secure link or internal compliance portal.

**Public Access (if applicable):**

If any portion of this Policy is published on the Company's official website, it shall be limited to general compliance principles and customer-facing obligations, excluding internal operational procedures or confidential elements.

**Internal Access:**

The full version of this Policy shall be available to all employees and contractors of Oxilium N.V. via the company's secure internal network or compliance management system. The most current approved version shall be maintained by the **Compliance Officer / MLRO** and referenced under the following internal link:

The MLRO shall ensure that:

- Outdated or unapproved versions are promptly removed from internal and external locations;
- Any publication of this Policy complies with the Company's confidentiality and data protection requirements;
- The Curaçao Gaming Authority (CGA) and other competent authorities have direct access to the most recent approved version upon request.