

OXILIUM N.V.

Know Your Customer (KYC) Policy

Version 2025.1

Document Classification: Internal / Regulatory Submission

Jurisdiction: Curaçao

License: Curaçao B2C Remote Gaming Operator (LOK framework / CGA regime)

Effective Date: 09/12/2025

Approved by: Board of Directors, Oxilium N.V.

Prepared by: Justice Nwankwo, AMLCO / MLRO

Next Review Date: [+12 months]

Confidentiality Notice: This document contains proprietary and confidential information belonging to Oxilium N.V. Unauthorised disclosure, distribution or reproduction is strictly prohibited. This Policy is subject to inspection by the Curaçao Gaming Authority (CGA), the Financial Intelligence Unit (FIU Curaçao), and other competent authorities.

Document Control & Revision History

Version	Date	Author	Description of Changes	Approved By
2025.1	09/12/2025	Justice Nwankwo	Initial issue of KYC Policy aligned with AML/CFT/CPF Regulations (Jan 2025)	Board of Directors

Document Status: Current Version: 2025.1

Owner: AMLCO / MLRO

Distribution: Internal (Compliance, Payments, Support), Regulatory (CGA, FIU)

Regulatory References

- AML/CFT/CPF Regulations (January 10, 2025)
- LOK 2024
- MOT & LID Legislation
- Sanctions Ordinance PB 2014 No. 55
- GCB Technical Standards 11, 12, 13
- FIU Curaçao goAML Requirements
- Oxilium N.V. AML/CFT/CPF Policy

Table of Contents

1. Introduction
 - 1.1 Purpose
 - 1.2 Scope
 - 1.3 Legal & Regulatory Basis
 - 1.4 Relationship with Other Policies
 - 1.5 Definitions
2. Risk-Based Approach (RBA)
3. Customer Identification (CDD Requirements)
4. Enhanced Due Diligence (EDD)
5. Customer Acceptance Policy (CAP)
6. Payment Methods & Financial Controls
7. Ongoing Monitoring
8. Sanctions Screening & TFS Controls
9. Suspicious Activity & Reporting (goAML)
10. Customer Communication Requirements
11. Recordkeeping & Data Retention
12. Governance & Responsibilities
13. Appendices

1. Introduction

This Know Your Customer (KYC) Policy establishes mandatory standards and procedures for identifying, verifying, assessing, and monitoring customers of Oxilium N.V. It forms an integral part of the Company's AML/CFT/CPF Compliance Framework and is fully aligned with the AML/CFT/CPF Policy dated 13 November 2025.

1.1 Purpose

The purpose of this Policy is to:

- Ensure compliance with all Curaçao legal and regulatory obligations.
- Implement consistent, risk-based onboarding and verification procedures.
- Prevent money laundering, terrorism financing, proliferation financing, sanctions violations, fraud, and misuse of the platform.
- Support accurate customer risk assessment and ongoing monitoring.
- Establish clear governance, reporting, and documentation requirements.

1.2 Scope

This Policy applies to all customers, all operational departments, and all payment channels (including fiat and crypto, where applicable). It governs onboarding, verification, monitoring, and risk management across the platform.

1.3 Legal & Regulatory Basis

This Policy is based on LOK 2024, AML/CFT/CPF Regulations (Jan 2025), MOT, LID, Sanctions Ordinance, FIU goAML obligations, and GCB Technical Standards, and the Process for the Freezing of Resources (2024 update), issued by the Ministry of Finance of Curaçao.

In the event of any conflict between this Policy and applicable laws, regulations, or binding regulatory guidance, the latter shall prevail. This Policy will be promptly updated to reflect any such changes.

1.4 Relationship with Other Policies

This Policy complements and must be read together with:

- AML/CFT/CPF Policy
- Operational Manual
- Information Security Policy
- Transaction Monitoring SOP
- Sanctions & TFS SOP
- Responsible Gaming Policy - Crypto Payments Addendum (if applicable)

Customer-facing implementation of this Policy is reflected in the Platform's Terms & Conditions, Privacy Notice, and other customer documentation, which must remain consistent with this Policy at all times.

1.5 Definitions

Key terms used in this Policy (including Customer Due Diligence, Enhanced Due Diligence, Politically Exposed Person, Risk-Based Approach, Unusual Transaction Report, goAML, Targeted Financial Sanctions, and related concepts) are defined in Appendix A (Definitions).

Where a term is already defined in the Oxilium N.V. AML/CFT/CPF Policy, that definition applies *mutatis mutandis* to this Policy, unless expressly stated otherwise herein.

2. Risk-Based Approach (RBA)

The Company adopts a comprehensive Risk-Based Approach in accordance with AML/CFT/CPF Regulations (January 2025), LOK 2024, FIU Curaçao guidance, and recognised industry standards. All customer verification, monitoring, and oversight measures are proportionate to the assessed level of ML/TF/PF risk.

2.1 Core Principles

- Proportionality: Higher-risk customers receive stricter controls, enhanced verification, and additional monitoring.
- Preventive Orientation: Focus on identifying risk at the earliest possible stage.
- Dynamic Assessment: Risk is reassessed continuously based on new data, transactions, behavioural indicators, and geographic factors.
- Full Documentation: All assessments must be recorded and available for CGA/FIU review.
- Consistency with AML Policy: RBA forms part of the overall AML/CFT/CPF Framework.

2.2 Customer Risk Categories

Customers are classified into the following tiers:

- Low Risk: Fully verified customers with predictable, low-volume activity and no risk indicators.
- Medium Risk: Standard customers with moderate activity and no EDD triggers.
- High Risk: Customers linked to high-risk jurisdictions, inconsistent behaviour, complex payment instruments, EDD triggers, or adverse screening results. High-risk customers require AMLCO approval before any withdrawals and prior to any material increase of transactional limits or other significant profile changes.

2.3 Customer Risk Assessment (CRA) Methodology

The CRA evaluates customers across five dimensions:

1. Geographical Risk: Residency, nationality, IP location, payment origin.
2. Customer Profile Risk: Age, occupation, PEP status, sanctions exposure, SOW/SOF.

3. Transactional Risk: Deposit velocity, patterns, unusual behaviour, sharp increases.
4. Behavioural & Product Risk: RG indicators, session patterns, fraud markers.
5. Payment Method Risk: Cards, e-wallets, transfers, crypto (if applicable), third-party payments.

Each element receives a score contributing to a final risk tier. Detailed scoring criteria for each risk dimension are set out in the Company's Customer Risk Assessment Methodology, which forms an integral part of the overall AML/CFT/CPF Framework.

2.4 Risk Ownership & Responsibilities

- AMLCO: Owns the framework, approves high-risk customers.
- Compliance Team: Conducts risk assessments, monitoring, and screening.
- Payments/Fraud: Identifies financial anomalies and escalates.
- Customer Support: Collects customer documentation upon instruction.
- Board of Directors: Ensures adequate resources for RBA implementation.

3. Customer Identification (CDD Requirements)

Customer Due Diligence (CDD) is mandatory for all customers of Oxilium N.V. and must be completed in accordance with AML/CFT/CPF Regulations, MOT and LID legislation, and FIU Curaçao requirements. No customer may be permitted to withdraw funds or exceed internal/regulatory deposit thresholds without successfully completing CDD as defined in this Policy. Basic registration data is collected at onboarding, while full verification is completed prior to first withdrawal or upon reaching defined thresholds, whichever occurs first.

3.A CDD Refresh Triggers

CDD must be refreshed when:

- Customer changes personal details (name, address, nationality)
- New payment methods are added
- Device/IP pattern changes significantly
- Customer reaches new transactional thresholds
- EDD triggers appear
- Long-term inactivity followed by sudden reactivation
- New adverse media appears
- New PEP or sanctions exposure is identified

3.1 Information Required at Registration

At the point of account creation, the Company must collect the following minimum information:

- ✓ Full legal name
- ✓ Date of birth
- ✓ Residential address
- ✓ Nationality

- ✓ Email address
- ✓ Mobile phone number
- ✓ Country of registration (must not be prohibited)
- ✓ Confirmation of age (18+)
- ✓ Acceptance of Terms & Conditions
- ✓ Acceptance of Privacy Policy
- ✓ Attestation of truthful information

The system must prevent account creation from prohibited jurisdictions.

3.2 Identity Verification Requirements

Before any withdrawal and prior to reaching regulatory thresholds, the customer must provide valid identification. Acceptable forms of ID include:

- Passport (ICAO-compliant)
- National ID card (government-issued)
- Driver's license (photo, full name, DOB)

ID must:

- Be valid and unexpired
- Clearly show required details
- Match registration information
- Be verified via approved KYC tools

If discrepancies or forgery indicators appear, the account must be suspended.

3.3 Proof of Address Requirements

Proof of address is required:

- Prior to first withdrawal
- For medium - and high-risk customers
- When triggered by EDD

Accepted documents (typically issued no more than 3 months prior to the date of submission, unless otherwise justified based on risk):

- Utility bill
- Bank statement
- Government correspondence

- Tax statement
- Lease agreement or property ownership proof

3.4 Payment Method Ownership Verification

The Company must verify that each payment method belongs to the customer:

- Bank Cards: Partial screenshot (first 6/last 4 digits), matching name
- Bank Transfers: Statement showing customer name and IBAN
- E-wallets: Screenshot confirming ownership
- Crypto (if applicable): Ownership via exchange account, wallet verification, or signed message

Third-party payments are strictly prohibited.

3.5 Corporate Customers (If Applicable)

This section applies only if corporate onboarding is permitted under the Company's licence conditions.

If corporate onboarding is allowed, the following documents are required:

- Certificate of Incorporation
- Shareholder/UBO Register
- UBO Identification
- Board Resolution
- Business activity proof, including a clear description of the intended use of the Company's services and expected transaction profile
- Jurisdictional FATF risk review

Corporate customers are automatically classified as high-risk.

3.6 Verification Before First Withdrawal

Before any withdrawal, the following must be verified:

- Identity document
- Proof of address (when required)
- Payment method ownership
- Transaction behaviour and patterns
- SOW/SOF (if EDD applies)
- Sanctions and PEP screening

No withdrawals may occur without full CDD and Compliance approval.

3.7 Regulatory thresholds

Thresholds are defined in the Company's Customer Risk Assessment Methodology and Deposit/Withdrawal Monitoring SOP and may be updated by AMLCO based on risk and regulatory guidance.

4. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is required for customers who present a higher ML/TF/PF risk or whose behaviour or documentation triggers additional scrutiny. EDD must be documented in full and approved by the AMLCO. Under no circumstances may EDD-required customers withdraw until the EDD process is completed and formally approved.

4.A Product / Channel-Based EDD

EDD must be applied where risk arises from:

- High-velocity or high-turnover gaming products
- Bonus abuse vectors or arbitrage behaviour
- Use of high-risk payment channels (e.g., unregulated e-wallets)
- Crypto-asset channels (if enabled)
- Unusual cross-product behaviour

4.1 Trigger Events (Event-Driven EDD)

EDD is initiated when any of the following triggers occur:

- Customer is linked to a high-risk jurisdiction (FATF, EU, Curaçao lists)
- Customer is identified as a Politically Exposed Person (PEP)
- Sanctions alerts (matches, potential matches, false positives requiring verification)
- Large or inconsistent deposits or withdrawals
- Sudden change in gambling or transactional behaviour
- Use of multiple payment methods or complex patterns
- Discrepancies in registration vs. verification information
- Crypto-asset transactions (if applicable)
- Attempts to circumvent limits, responsible gaming controls, or monitoring
- Multiple accounts, shared devices, VPN/proxy use
- Rejected or inconsistent documents
- Refusal to provide SOF/SOW

Any trigger event must be recorded in the Compliance Log.

4.2 EDD for High-Risk Jurisdictions

Customers connected to jurisdictions classified as high-risk by FATF or Curaçao authorities are automatically subject to EDD.

Required actions:

- Obtain additional identity verification
- Obtain SOF/SOW documentation
- Verify payment method ownership with additional proof
- Validate geographical information (IP, device, behavioural patterns)
- Perform enhanced sanctions & PEP screening
- Obtain AMLCO approval

4.3 EDD for PEPs & Sanctions Alerts

Politically Exposed Persons (PEPs)

EDD must include:

- Identification of PEP type (domestic, foreign, international organisation)
- Identification of Close Associates and Family Members
- SOF/SOW documentation
- Senior-level approval (AMLCO)
- Transaction monitoring on a continuous basis

Sanctions Alerts

If a sanctions alert appears:

- Immediate account freeze (if match is confirmed)
- Verification of potential false positive
- Escalation to AMLCO
- Reporting to FIU if required

4.4 EDD for High-Value Transactions

EDD is required for:

- Large or irregular deposits/withdrawals
- Repeated high-value transactions
- Patterns inconsistent with customer profile
- Third-party payment attempts

EDD must include a clear assessment of whether the activity is:

- Economically reasonable
- Supported by SOF/SOW
- Free of ML/TF/PF indicators

4.5 EDD for Crypto-Asset Transactions (If Applicable)

If crypto is used as a payment method, EDD must include:

- Verification of wallet ownership
- Source of crypto funds (exchange account, on-chain data if needed)
- Sanctions and darknet exposure screening using approved tools
- Transaction pattern analysis
- Additional documentation if behaviour triggers red flags.

The Company performs blockchain analytics to a proportional extent required by risk level and FIU/CGA guidance, using approved tools/providers. As a minimum, sanctions, darknet exposure, and high-risk wallet indicators must always be screened for relevant crypto transactions. Full-scale on-chain tracing is applied only where necessary under EDD, in accordance with FIU Curaçao guidance and the Company's risk assessment.

4.5.1 Event-Driven EDD Escalation Chain

Event-Driven EDD applies when an unexpected behavioural, transactional, or screening trigger arises outside the normal CDD process. When a trigger occurs, the escalation sequence is:

1. The system or staff detect a trigger event.
2. Compliance performs preliminary review and determines whether immediate account restrictions are necessary.
3. If concerns remain, Compliance opens a formal EDD case and temporarily suspends withdrawals.
4. AMLCO conducts a full review of documents, activity consistency, risk indicators, and SOF/SOW.
5. AMLCO issues a final decision: approve, approve with restrictions, continue monitoring, or terminate the relationship.
6. If activity appears suspicious, MLRO files a UTR/STR to FIU Curaçao through goAML without tipping off the customer.

All Event-Driven EDD cases must be recorded in the Compliance Log.

4.6 Source of Funds (SOF) / Source of Wealth (SOW)

When SOF/SOW is required, the customer must provide:

- Employment confirmation or payslip
- Bank statements showing legitimate income
- Proof of business ownership (if applicable)
- Inheritance, asset sale, or other supporting documentation
- Crypto exchange statements (if applicable)

SOF/SOW must:

- Support the customer's observed activity
- Be independently verifiable
- Be retained in the customer's file
- Be approved by the AMLCO

4.7 Counter-Proliferation Financing (CPF) Procedure

Oxilium N.V. incorporates Counter-Proliferation Financing controls as part of its AML/CFT/CPF framework. CPF risk is addressed through sanctions screening, TFS controls, and jurisdictional risk assessment in accordance with Curaçao AML/CFT/CPF Regulations (January 2025), the Sanctions Ordinance (PB 2014 No. 55), and FATF Recommendation 7.

CPF safeguards include:

The Company screens all customers, payment methods, devices, and relevant counterparties against sanctions lists identifying individuals or entities involved in proliferation activities. Any confirmed or potential match triggers immediate suspension of the customer account, a freeze of resources in accordance with "Process for the Freezing of Resources", and escalation to the AMLCO for determination of reporting obligations to FIU Curaçao.

CPF is also embedded in jurisdictional risk analysis. Customers with direct or indirect connections to high-risk or proliferation-linked jurisdictions are subject to EDD and may be refused service where the risk cannot be mitigated.

At this stage, CPF risks are primarily mitigated through sanctions screening, TFS implementation, jurisdictional risk assessment, and EDD. The Company will introduce additional standalone CPF controls if and when required by changes in its risk exposure or regulatory guidance. However, Compliance must remain vigilant in detecting patterns consistent with proliferation financing typologies, including unusual trade-style transfers, structured movement of funds, or use of high-risk intermediaries.

All CPF-related alerts must be escalated to the AMLCO and handled using the same escalation chain as sanctions-related events.

5. Customer Acceptance Policy (CAP)

The Customer Acceptance Policy defines the criteria under which Oxilium N.V. may onboard, restrict, or decline customers. CAP ensures compliance with Curaçao legislation, FATF standards, and the Company's AML/CFT/CPF Framework. No customer may participate if they fall under a prohibited category listed in this section.

5.1 Prohibited Jurisdictions

The Company strictly prohibits onboarding or servicing customers who are:

- ✓ Residents or nationals of jurisdictions classified as high-risk or subject to a call for action by FATF
- ✓ Residents of jurisdictions sanctioned by the UN, EU, OFAC, or Kingdom of the Netherlands
- ✓ Located in territories where online gaming is illegal or prohibited
- ✓ Using VPNs or proxies to mask location from prohibited jurisdictions. Where the use of VPN or proxy reveals access from a prohibited jurisdiction, the account must be suspended, and any funds handled in accordance with applicable laws, CGA guidance, and this Policy.

If a customer is found to be from a prohibited jurisdiction, the account must be immediately suspended and escalated to AMLCO. The company shall follow the Curaçao Gaming Authority Circular "Prohibited Jurisdictions List", as updated from time to time.

The AMLCO is responsible for maintaining and updating the internal Prohibited and Restricted Jurisdictions Lists, reflecting FATF publications, CGA circulars, sanctions updates, and other relevant regulatory sources.

5.2 Restricted Jurisdictions

Customers from jurisdictions classified as increased monitoring / grey-listed by FATF, or considered higher-risk under Curaçao regulations, may be accepted only under:

- Full CDD verification
- Mandatory EDD
- SOF/SOW documentation
- AMLCO approval prior to withdrawals

Their activity must be subject to enhanced ongoing monitoring.

5.3 High-Risk Customer Profiles

Customers classified as high-risk include:

- PEPs and their close associates or family members
- Customers demonstrating inconsistent or unusual transaction patterns
- Customers with complex payment behaviours
- Crypto-users (if crypto is accepted)

- Customers linked to high-risk jurisdictions
- Corporate customers (if applicable)

High-risk customers require AMLCO approval for onboarding and withdrawals.

5.4 PEP Acceptance Standards

The Company may onboard PEPs only under:

- Mandatory EDD
- Verification of PEP status and associates
- SOF/SOW documentation
- Continuous monitoring of transactions
- AMLCO approval

Any PEP refusal or acceptance decision must be documented.

5.5 Sanctioned Individuals

The Company must refuse and/or immediately terminate access if a customer is:

- Listed on sanctions lists (UN, EU, OFAC, Kingdom of the Netherlands)
- Closely associated with sanctioned individuals or entities
- Attempting to circumvent sanctions through intermediaries or VPNs

Confirmed matches require:

- Immediate account freezing
- AMLCO escalation
- Regulatory reporting (FIU/goAML)

5.6 Anonymous or Unverified Accounts

The Company does not permit:

- Anonymous accounts
- Accounts with incomplete registration data
- Accounts that have not completed mandatory CDD

Such accounts must be suspended until verification is completed.

Customers under 18 years of age or subject to self-exclusion / regulatory exclusion are prohibited and must be blocked at onboarding and on an ongoing basis.

5.7 Third-Party Payments

The Company prohibits:

- Deposits or withdrawals through third-party financial instruments
- Use of cards, e-wallets, or bank accounts not owned by the customer
- Shared wallets or accounts

Any detected third-party payment attempt triggers:

- Immediate suspension
- EDD - AMLCO review
- Possible STR/UTR to FIU Curaçao

6. Payment Methods & Financial Controls

The Company must ensure that all payment channels comply with Curaçao AML/CFT/CPF Regulations (January 2025), FATF Recommendations, and the Company's internal AML Policy. All payment methods must undergo ownership verification, monitoring, and risk assessment. Third-party transactions are strictly prohibited.

6.1 Approved Fiat Payment Methods

Oxilium N.V. accepts only payment methods that permit full ownership verification and traceability. Approved fiat channels include:

- Bank cards (Visa/Mastercard)
- Bank transfers (SEPA/SWIFT)
- E-wallets (approved providers only)
- Local payment rails (only after AMLCO approval)

Requirements:

- ✓ Payment service providers must be vetted and approved by AMLCO
- ✓ All payment flows must be monitored for anomalies
- ✓ Cards and accounts must belong to the customer

The AMLCO must ensure that each payment service provider is subject to initial and periodic due diligence, covering licensing status, jurisdictional risk, AML and sanctions controls, and any adverse regulatory or media findings.

6.2 Payment Method Ownership Verification

Before processing withdrawals, the Company must confirm that the payment method is owned by the customer.

Verification requirements:

- Bank Cards: Partial screenshot showing first 6 / last 4 digits and customer name
- Bank Transfers: Statement showing name and IBAN

- E-wallets: Ownership screenshot
- Prepaid Cards: Not accepted (unless AMLCO approves in exceptional, duly documented cases with a clear risk mitigation rationale)

Any mismatch leads to account suspension and EDD.

6.3 E-Wallets

Accepted only if:

- The e-wallet is fully traceable
- Ownership is verifiable
- Provider is not based in a high-risk jurisdiction

E-wallet use triggers a medium-risk rating unless EDD clears concerns.

6.4 Crypto-Asset Payments (If Applicable)

If the Company accepts crypto payments, the following applies:

- Only approved crypto payment processors may be used - BTC, ETH, USDT, or other AMLCO-approved assets
- Wallet ownership must be verified through:
 - Exchange statement
 - Wallet ownership proof
 - Blockchain transaction evidence (proportionate screening)

Prohibited:

- Privacy coins
- P2P transfers without verification
- Mixing/tumbling services

All crypto transactions require behavioural monitoring and EDD if red flags arise.

6.5 Deposit & Withdrawal Risk Controls

The Company must implement controls to detect irregular payment behaviour, including:

- High-velocity deposits
- Repeated failed transactions
- Rapid deposit-withdrawal cycles
- Use of multiple cards/wallets
- Unusual time patterns

- Geographic inconsistency (IP vs. payment origin)

Controls include:

- Automated alerts
- Compliance review
- Temporary suspension until clarified

6.6 Third-Party Payment Restrictions

The Company strictly prohibits:

- Deposits made using payment instruments owned by another person
- Withdrawals to third-party accounts
- Accounts used by multiple individuals

Detected third-party activity requires:

- Immediate suspension
- EDD
- AMLCO review
- Possible FIU reporting

6.7 Failed & Attempted Transactions

The Company must log and review failed or attempted transactions as required by MOT legislation.

Attempted third-party payments or attempts to bypass payment rules must trigger Compliance review.

7. Ongoing Monitoring

Ongoing Monitoring is a mandatory requirement under Curaçao AML/CFT/CPF Regulations (January 2025). It ensures continuous oversight of customer behaviour, transactional activity, and compliance with all AML, CFT, CPF, and sanctions obligations. The Company must detect changes in customer risk profile, patterns indicative of ML/TF/PF, and inconsistencies requiring escalation.

7.A Integration of AML and Responsible Gaming (RG)

Oxilium N.V. recognises that AML and Responsible Gaming share overlapping behavioural indicators. Certain RG-related patterns, including loss-chasing, sudden risk-seeking activity, or attempts to circumvent limits, may also indicate elevated AML/TF/PF risk.

Compliance and Responsible Gaming teams maintain a coordinated information-sharing mechanism. Any RG escalation involving financial anomalies must be reviewed by Compliance for possible AML implications. Likewise, AML-detected behavioural irregularities may be forwarded to RG when indicators of harm or vulnerability are present.

This integration ensures a comprehensive, multi-layered view of customer risk and aligns with CGA expectations. This cooperation is formalised through joint procedures and shared escalation channels between the AML/Compliance function and the Responsible Gaming function.

7.1 Transaction Monitoring

The Company must monitor all transactions for unusual or suspicious patterns. Automated and manual monitoring must detect:

- Rapid deposit-withdrawal sequences
- High-value transactions inconsistent with profile
- Use of multiple payment methods
- Geographic inconsistencies
- Dormant accounts suddenly becoming active
- Attempted third-party transactions
- Irregular crypto activity (if applicable)

Alerts must be escalated to Compliance for review. All monitoring alerts (automated and manual) must be recorded with timestamps, reviewer identity, and resolution outcome in the Compliance Log.

The Company's monitoring scenarios and red-flag indicators are aligned with FIU Curaçao Indicators of Unusual Transactions (MOT typologies) and updated accordingly.

7.2 Behavioural Monitoring

Behavioural indicators must be continuously monitored, including:

- Irregular gameplay patterns
- Excessive session duration
- Attempts to bypass limits or controls
- Risky or compulsive gameplay (integration with RG team)
- Device/Browser changes inconsistent with customer profile

Behavioural red flags may trigger EDD or suspension.

7.2.A Event-Driven Re-Scoring

Any trigger event (behavioural, transactional, sanctions, device, RG, payment) must result in:

- a. immediate CRA recalculation;
- b. adjustment of risk tier;
- c. updated monitoring frequency.

Event-driven re-scoring must be performed as soon as practicable and, in any event, within three (3) business days from detection of the trigger event, in line with internal procedures approved by the AMLCO.

7.3 Device, IP & Geolocation Monitoring

The Company must monitor:

- IP addresses
- Device IDs
- Geolocation data
- VPN/Proxy/Tor usage

Red flags include:

- Frequent IP changes
- Logins from prohibited or high-risk jurisdictions
- Geo-location mismatches with payment origin
- Shared devices across multiple accounts

Any such behaviour triggers compliance review.

7.4 Monitoring Frequency by Risk Tier

Monitoring intensity is based on customer risk rating:

- Low-risk: Standard automated monitoring
- Medium-risk: More frequent behavioural and transactional review
- High-risk: Continuous monitoring with manual review

High-risk customers require AMLCO approval for withdrawals.

7.5 Cross-Functional Escalation (RG/Fraud/Payments)

Compliance must collaborate with:

- Fraud: to identify suspicious transactional or technical patterns
- Responsible Gaming: to detect financial vulnerability indicators
- Payments: to review payment method inconsistencies
- Customer Support: to capture customer communication red flags

Information sharing must follow internal confidentiality rules.

7.6 Periodic Review

Every active customer must undergo periodic reassessment:

- ✓ Low-risk: every 24 months
- ✓ Medium-risk: every 12 months
- ✓ High-risk: every 6 months or upon any trigger event

Reviews include:

- Updated screening (PEP, sanctions)
- Behavioural history
- Transaction patterns
- Payment activity
- Documentation updates if required

8. Sanctions Screening & TFS Controls

The Company must comply with all applicable sanctions regimes, including those issued by the United Nations, European Union, OFAC, and the Kingdom of the Netherlands. In accordance with the Sanctions Ordinance (PB 2014 No. 55), AML/CFT/CPF Regulations, and the “Process for the Freezing of Resources,” the Company must conduct sanctions screening at onboarding, continuously thereafter, and upon any trigger event.

8.1 Initial Screening

All customers must be screened at registration against:

- UN Consolidated List
- EU Sanctions List
- OFAC SDN List
- Kingdom of the Netherlands Sanctions Lists
- Internal high-risk and prohibited jurisdiction lists

Screening must be automated where possible. Manual review is required for potential matches.

8.2 Continuous Screening

Continuous screening must be performed to detect:

- Newly sanctioned individuals
- Changes in customer PEP/sanctions status
- Activity suggesting sanctions evasion
- Crypto wallet exposure to sanctioned entities (if applicable)

Any positive match must immediately pause the account pending review.

Alerts or notices received from PSPs/banks indicating sanctions exposure or evasion attempts are treated as trigger events requiring immediate Compliance review.

8.3 Freezing of Assets

If a sanctions match is confirmed:

- The customer account must be frozen immediately
- No transactions may be processed
- No funds may be released without regulatory approval.

Actions must follow the requirements in:

- Sanctions Ordinance (PB 2014 No. 55)
- FIU Curaçao guidance - “Process for the Freezing of Resources.”

Freezing must include the prevention of all outward and inward transactions, including bonuses and non-monetary credit.

8.4 Escalation to AMLCO

All sanctions alerts must be escalated to the AMLCO, who must:

- Review the alert
- Confirm or dismiss the match
- Classify it as “true match” or “false positive”
- Document the decision
- Trigger reporting if required

AMLCO approval is mandatory before unfreezing or closing the account.

AMLCO decisions on sanctions-related cases must be retained for a minimum of 10 years (FIU requirement).

8.5 Non-Tipping-Off Requirements

Staff must not disclose:

- That a customer is under sanctions investigation
- That a report is being prepared or submitted to FIU
- That screening results triggered internal actions

Any disclosure is prohibited and constitutes a regulatory breach.

8.6 Reporting Requirements

If a sanctions match or attempted sanctions evasion is confirmed:

- An Unusual Transaction Report (UTR/STR) must be filed via goAML
- Documentation must be retained
- Authorities must be provided full cooperation

Reporting must follow formats defined by FIU Curaçao and obligations under MOT.

9. Suspicious Activity & Reporting (goAML)

The Company must identify, assess, document, and report unusual or suspicious activity in accordance with:

- AML/CFT/CPF Regulations
- MOT Legislation
- FIU Curaçao guidance
- goAML reporting standards
- The Company's AML/CFT/CPF Policy

Suspicious activity must be escalated internally and, where required, reported externally to FIU Curaçao via the goAML portal.

9.1 Internal Suspicious Reports (ISR)

Any employee who identifies or suspects unusual or suspicious activity must immediately file an Internal Suspicious Report (ISR) to Compliance.

Indicators include:

- Sudden large or irregular deposits/withdrawals
- Payments inconsistent with SOF/SOW
- Attempts to bypass verification or monitoring
- Use of multiple accounts, devices, or identities
- Crypto transactions with high-risk exposure (if applicable)
- Links to high-risk jurisdictions or sanctioned entities
- Behavioural anomalies suggesting ML/TF/PF

ISRs must be logged and retained.

9.2 MLRO Assessment

Upon receiving an ISR, the AMLCO/MLRO must:

- Conduct a detailed assessment
- Review transactional and behavioural data

- Examine customer documentation
- Perform sanctions and PEP checks
- Determine whether the activity meets the threshold for reporting
- The MLRO must document the decision as:
 - Reportable (UTR/STR), or
 - Not reportable, with justification

9.3 goAML Submission

If the MLRO determines that the case is reportable, an Unusual Transaction Report (UTR/STR) must be submitted to FIU Curaçao through the goAML system.

Mandatory requirements:

- Submission must be timely (as soon as practicable)
- All relevant data must be included
- Supporting documents must be attached
- The customer must not be informed (non-tipping-off)

Account status during reporting:

- If sanctions-related → immediate freeze
- If ML/TF suspicion → temporary freeze or AMLCO-directed restrictions

9.4 Documentation Standards

All ISR and STR/UTR cases must include:

- Detailed narrative of behaviour
- Timeline of events
- Screenshots, documents, and logs
- Transaction history
- AMLCO decision and rationale
- Actions taken (e.g., freeze, suspension)

Records must be stored securely and accessible for CGA/FIU review.

9.5 Reporting Timelines

The Company must follow FIU Curaçao requirements:

- ✓ Reports must be filed without delay once suspicion is confirmed, and
- ✓ All internal reviews must be logged with timestamps.

Delays in reporting constitute a regulatory breach. Breach of non-tipping-off requirements in the context of suspicious activity assessment and goAML reporting constitutes serious misconduct and may lead to disciplinary measures, up to and including termination of employment, without prejudice to any regulatory or criminal consequences.

10. Customer Communication Requirements

All communication with customers regarding verification, documentation, account status, or compliance actions must adhere to AML/CFT/CPF Regulations, non-tipping-off rules, data protection principles, and the Company's AML/CFT/CPF Policy. Communications must be clear, professional, and must never disclose assessments or reporting obligations.

10.1 Requests for Additional Documentation

When additional documents are required (CDD or EDD), Compliance or Customer Support must:

- Request documents in a neutral, non-accusatory tone
- Specify acceptable document types
- Provide secure submission channels
- Avoid providing reasons that could constitute tipping-off

Example acceptable wording:

“Thank you for your cooperation. To complete your account verification, we kindly ask you to provide the following document(s). This is a standard requirement for account processing.”

10.2 EDD Requests

If Enhanced Due Diligence is required, communication must:

- Avoid referencing risk flags or suspicions
- Avoid referencing sanctions, PEP status, ML/TF concerns
- Encourage timely submission

Example wording:

“To finalise your verification, we require additional documentation. Please provide the following documents so we may proceed.”

10.3 Account Suspension Notices

If an account is temporarily restricted:

- Do not mention suspicious activity or reporting
- Provide a neutral reason
- Keep language procedural

Example wording:

“Your account has been temporarily restricted pending routine verification. Please provide the requested documents so we can restore full access.”

10.4 Account Closure Notices

If the Company decides to terminate the relationship:

- Do not provide detailed reasons
- Do not mention ML/TF suspicion or STR filing
- Maintain neutral, compliance-based language

Example wording:

“Following an internal review, we will not be able to continue offering services to you. Your account will be closed in accordance with our Terms & Conditions. Remaining funds will be returned to your verified payment method where applicable.”

10.5 Standard Non-Tipping-Off Wording

In all communications related to verification or restrictions, the following principles apply:

- Never reference internal monitoring systems
- Never reference FIU Curaçao or goAML
- Never reference “suspicious,” “AML,” “investigation,” “risk,” or similar language
- Use generic, procedural explanations only

Approved standard statements:

- “Your account is undergoing routine review.”
- “We require additional documentation to complete verification.”
- “Your withdrawal is pending standard compliance checks.”
- “We appreciate your cooperation during this process.”

Any customer complaints arising from verification processes, account restrictions, or closures must be handled in accordance with the Company’s Complaints Handling Policy, without prejudice to the non-tipping-off obligations set out in this Policy.

11. Recordkeeping & Data Retention

The Company must maintain complete, accurate, and secure records in accordance with AML/CFT/CPF Regulations, MOT and LID requirements, Sanctions Ordinance PB 2014 No. 55, GCB Technical Standards, and FIU Curaçao expectations. Records must be readily accessible for inspection by the Curaçao Gaming Authority (CGA), FIU Curaçao, and other competent authorities.

All access to customer files must be logged and subject to audit trail requirements under AML/CFT/CPF Regulations.

All recordkeeping and data retention activities under this Policy must be carried out in compliance with applicable data protection and privacy laws, including any GDPR-equivalent obligations where relevant.

11.1 Minimum Retention Period

All AML/CFT/CPF and customer verification records must be retained for a minimum of five (5) years after:

- The customer relationship has ended, or
- The date of the last transaction, whichever is later.

The retention period applies to:

- CDD/EDD documents
- Payment method ownership proofs
- SOF/SOW documentation
- Transaction histories
- Sanctions & PEP screening logs
- Internal Suspicious Reports (ISR)
- FIU goAML submissions (UTR/STR)
- Communications with customers
- Compliance decision logs
- Monitoring alerts and reviews

Notwithstanding the general five (5) year retention period, sanctions-related decisions and documentation (including AMLCO decisions referred to in Section 8.4) may be retained for longer periods, up to ten (10) years or more, where required by FIU Curaçao or other applicable regulations.

11.2 Storage & Archiving

Records must be stored:

- Securely
- In encrypted environments
- With role-based access controls
- With audit trails tracking access and modifications. Audit trails must, at a minimum, capture the user ID, timestamp, type of access (view, edit, export), and, where applicable, the justification for access

Acceptable storage options:

- Secure internal servers
- Encrypted cloud storage compliant with data protection standards

Unacceptable:

- Personal devices
- Unencrypted external drives
- Email-only storage

11.3 Access Control

Access to sensitive information must be limited to:

- AMLCO / MLRO
- Compliance Team members
- Auditors (internal and external)
- Regulatory authorities

Other employees may only access information if explicitly required for operational purposes and approved by AMLCO.

11.4 Regulatory Requests

The Company must be able to provide any of the following to regulators without undue delay:

- Customer identification files
- Transaction data
- Monitoring logs
- EDD assessments
- Sanctions screening results
- goAML submission evidence
- Policy and procedure documents

All regulatory requests must be recorded in the Regulatory Interaction Log.

12. Governance & Responsibilities

Effective governance is essential for ensuring compliance with Curaçao AML/CFT/CPF Regulations 2025, LOK 2024, FIU Curaçao requirements, and internal Company policies. This section defines the roles, duties, and accountability structure within Oxilium N.V.

12.1 Board of Directors

The Board holds ultimate responsibility for the Company's compliance framework. Duties include:

- Approving AML/CFT/CPF and KYC Policies
- Ensuring adequate staffing and resources for Compliance
- Overseeing the AMLCO/MLRO appointment
- Reviewing compliance reports and audit findings
- Ensuring corrective actions are implemented

The Board must demonstrate awareness of ML/TF/PF risks and foster a culture of compliance.

12.2 AMLCO / MLRO

The AMLCO/MLRO is the primary responsible officer for AML/CFT/CPF compliance. Responsibilities include:

- Maintaining and updating all compliance policies
- Supervising CDD/EDD processes
- Reviewing monitoring alerts and ISR submissions
- Approving high-risk customers and EDD outcomes
- Overseeing sanctions screening and frozen assets procedures
- Filing UTR/STR reports through goAML
- Providing training to employees
- Ensuring compliance with audits and regulatory inspections

The AMLCO must operate independently and have access to all necessary data. The AMLCO must have unrestricted access to all customer data, monitoring systems, and payment information, and must operate free from operational and commercial influence.

For the purpose of this Policy, the roles of AMLCO and MLRO may be combined and performed by the same individual, subject to CGA approval and fit-and-proper requirements. Where the roles are separated, the responsibilities set out in this Policy apply to each respective role as specified in the Company's AML/CFT/CPF Framework.

12.3 Compliance Team

The Compliance Team supports AMLCO by:

- Conducting CDD/EDD reviews
- Monitoring transactions and behaviour
- Performing screening (PEP, sanctions)
- Maintaining documentation and audit trails

- Escalating suspicious cases to AMLCO
- Assisting during regulatory audits

Compliance staff must maintain competence, confidentiality, and objectivity.

12.4 Payments & Customer Support

These departments must:

- Perform preliminary checks on deposits and withdrawals
- Collect documentation as instructed by Compliance
- Escalate anomalies or user claims immediately
- Follow non-tipping-off rules

They must not make independent risk decisions without Compliance direction.

12.5 Fraud & Risk Team

Where applicable, the Fraud/Risk team must:

- Identify technical or behavioural fraud indicators
- Monitor devices, velocity, and transaction anomalies
- Cooperate with Compliance on escalations

12.6 Information Security & IT

Information Security/IT must:

- Maintain secure systems for data retention
- Implement access controls and monitoring
- Support secure data transmission and storage
- Assist in investigations requiring system logs or device analytics

12.7 Internal & External Audit

Audit functions must:

- Review AML/CFT/CPF controls
- Test the efficiency of monitoring tools
- Examine adherence to policies
- Report findings to the Board

12.8 Policy Review Schedule

This Policy must be reviewed:

- At least annually
- After major regulatory changes
- After internal/external audit recommendations
- After material changes in business model

Any amendments require Board approval.

13. Appendices

The following appendices form an integral part of the KYC Policy and provide operational detail, definitions, and supplementary tools required for full compliance with Curaçao AML/CFT/CPF Regulations 2025, FIU Curaçao directives, and Oxilium N.V.'s AML Framework.

Appendix A - Definitions

This appendix provides clear definitions of key terms used throughout the Policy. All definitions reflect Curaçao AML/CFT/CPF Regulations 2025, MOT, LID, FIU Curaçao guidance, and international standards (FATF).

Adverse Media: Publicly available information linking a customer to potential financial crime, fraud, sanctions, corruption, or other illegal activity.

Business Relationship: A business, professional, or commercial relationship between the Company and a customer which is expected, at the time when contact is established, to have an element of duration.

Customer: Any natural or legal person who has registered an account with the Company and/or uses the Company's services.

Customer Due Diligence (CDD): Mandatory process of identifying and verifying a customer before allowing financial activity.

CDD Refresh: Re-verification of customer identity and risk triggered by regulatory requirements, internal thresholds, or behavioural changes.

Enhanced Due Diligence (EDD): Additional verification applied to customers presenting higher ML/TF/PF risk.

Politically Exposed Person (PEP): An individual holding (or having held) prominent public functions, including close associates and family members.

Sanctions Match: Confirmed match with UN, EU, OFAC, or Dutch sanctions lists requiring account freeze.

Potential Match: A screening alert requiring manual review to confirm or dismiss the match.

Source of Funds (SOF): Origin of funds used for transactions (e.g., salary, business income, savings).

Source of Wealth (SOW): The origin of a customer's total accumulated wealth.

High-Risk Customer: A customer whose aggregated risk score falls within the "High Risk" range under the CRA Matrix and/or who meets any of the high-risk criteria defined in Section 5.3 of this Policy.

High-Risk Jurisdiction: A country listed on FATF's call-for-action or grey list, or classified as high-risk by Curaçao authorities.

Unusual Transaction Report (UTR/STR): A report submitted to FIU Curaçao when a transaction or activity is deemed unusual or suspicious.

goAML: Official reporting system used for electronic submission of STR/UTR to FIU Curaçao.

Risk-Based Approach (RBA): Framework ensuring that controls are proportional to assessed customer risk.

Beneficial Owner (UBO): Natural person who ultimately owns or controls a legal entity.

Crypto-Asset (if applicable): A digital asset (e.g., BTC, ETH) used for payments when approved by the Company.

Mixing/Tumbling Services: Tools designed to obscure the origin of crypto transactions; strictly prohibited.

Targeted Financial Sanctions (TFS): Regulatory obligations requiring the identification, blocking, and freezing of assets belonging to individuals or entities listed under UN, EU, OFAC, or Dutch sanctions regimes.

Third-Party Payment: Any payment made using a method not owned by the customer; strictly prohibited.

Non-Tipping-Off: Legal requirement prohibiting disclosure of AML or sanctions investigations to customers.

Behavioural Monitoring: Continuous monitoring of customer activity patterns to detect anomalies.

Freezing of Resources: Immediate action required when a sanctions match is confirmed.

Internal Suspicious Report (ISR): Internal escalation filed by an employee when suspicious activity is detected.

FATF: Financial Action Task Force - international body setting global AML/CFT standards.

Appendix B - Customer Document Acceptance Table

This table outlines acceptable and unacceptable customer documents.

Identity Documents (ID):

- Accepted: Passport, National ID, Driver's License (photo, DOB)

- Not Accepted: Student IDs, Work IDs, Expired IDs

Proof of Address (POA):

- Accepted: Utility bill, Bank statement, Tax letter, Government letter (≤ 3 months)
- Not Accepted: Mobile top-up receipts, handwritten letters

Payment Method Proof:

- Cards: Partial screenshot (first 6 / last 4 digits)
- Bank: Statement with name + IBAN
- E-wallets: Ownership screenshot
- Crypto (if applicable): Exchange statement or wallet proof

All documents must be clear, legible, complete, and free from visible editing. The full document must be visible (no cropping), and scans or photos must be of sufficient resolution to allow reliable verification. The Company may reject any document that does not meet these standards.

Appendix C - CRA (Customer Risk Assessment) Matrix

This matrix defines how customers are assigned Low/Medium/High risk tiers.

Risk Dimensions:

1. Geographical Risk (0–3)

2. Customer Profile Risk (0–3)
3. Transactional Risk (0–3)
4. Behavioural Risk (0–3)
5. Payment Method Risk (0–3)

Risk Tier Calculation:

- Low Risk: 0–4 points
- Medium Risk: 5–7 points
- High Risk: 8+ points

Risk tier determines monitoring frequency, EDD requirements, and AMLCO approval steps.

Appendix D - SOF/SOW Documentation Table

Acceptable supporting evidence for SOF/SOW:

- Salary: Payslips, employment letter
- Business Income: Company documents, invoices, bank statements

- Savings: Bank history covering relevant period
- Crypto (if applicable): Exchange statements, wallet evidence
- Inheritance/Assets: Legal paperwork, sale contracts

Unacceptable evidence:

- Cash screenshots
- Edited or unverifiable documents

Appendix E - Trigger Events (Full List)

Trigger events requiring Compliance review, EDD, or AMLCO escalation include:

Identity Issues: unverifiable, manipulated, or inconsistent documents; repeated failed verification attempts; repeated requests to change core personal data (such as name, date of birth, or residential address) without a reasonable and verifiable justification.

Payment & Transaction Issues: rapid deposit-withdrawal patterns, multiple payment methods, high-value transactions inconsistent with profile, attempted third-party payments, chargebacks.

Behavioural Issues: use of VPN/Proxy/Tor, device or IP anomalies, sudden spikes in activity, attempts to bypass limits or verification.

Sanctions & PEP Issues: potential or confirmed match, newly detected PEP status, adverse media exposure.

Jurisdictional Issues: logins from high-risk or prohibited jurisdictions, payment methods originating from elevated-risk regions.

SOF/SOW Issues: income inconsistent with activity, refusal to provide SOF/SOW, unverifiable financial explanations.

Unusual device fingerprint patterns: device characteristics inconsistent with the customer's prior profile or linked to multiple unrelated accounts, potentially indicating identity manipulation, fraud, or ML/TF/PF concealment.

Multiple account creation attempts: repeated registration attempts from the same device, IP, or user identity, suggesting account manipulation or suspicious behaviour.

Sudden change in deposit method or gambling product: abrupt financial or gameplay changes inconsistent with historical patterns, requiring EDD and AMLCO review.

Appendix F — Escalation Flowcharts

CDD/EDD Flow:

Registration → CDD → (Trigger) Event-Driven EDD → AMLCO Decision → Approve / Approve with Restrictions / Decline / Offboard → (If suspicious) goAML.

Sanctions Flow:

- Screening Alert → Compliance Review → False Positive → continue monitoring.
- Possible Match → Account Freeze → AMLCO Review → Confirmed Match → goAML + resource freezing.
- Dismissed → unfreeze with monitoring.

Suspicious Activity Flow:

- Internal Suspicious Report → Compliance Review → AMLCO Assessment → STR/UTR via goAML
- Not Reportable (documented) → continue monitoring.

Appendix G - Prohibited & Restricted Jurisdictions

Prohibited jurisdictions include: FATF High-Risk jurisdictions (“Call for Action”), countries under UN/EU/OFAC/Dutch sanctions, jurisdictions where online gaming is illegal, countries prohibited by the Curaçao Gaming Authority, and any location masked by VPN/Proxy indicative of prohibited geography.

Restricted jurisdictions include FATF Grey-Listed countries and countries with elevated ML/TF/PF exposure. Customers from restricted jurisdictions may be accepted only after full CDD, mandatory EDD, SOF/SOW verification, AMLCO approval, and enhanced monitoring.

Lists must be updated after each FATF plenary and regulatory circular.

The Company also prohibits customers attempting to onboard from jurisdictions indirectly connected to prohibited regions through payment instruments, devices, or IP infrastructure.

The Company must implement automated real-time blocking for login attempts or payments originating from prohibited jurisdictions.

Appendix H - Crypto Addendum (If Applicable)

If Oxilium N.V. supports crypto payments, this appendix defines:

- Accepted crypto assets
- Approved processors
- Ownership verification steps
- Transaction screening rules
- Prohibited activities (mixing, privacy coins, P2P unverified transfers)

This appendix activates only if crypto is enabled operationally.

Blockchain analytics must be applied proportionally to risk, but always at least at the level required to ensure sanctions and darknet exposure screening.

Appendix I - Sanctions & TFS SOP Summary

Summary of operational steps for:

- Screening workflows
- Confirmed sanctions matches
- Freezing of resources
- Internal documentation
- Reporting via goAML.

This SOP aligns with:

- Sanctions Ordinance PB 2014 No. 55
- The Process for the Freezing of Resources
- AML/CFT/CPF Regulations 2025.

All sanctions-related decisions must be documented with timestamps, including freeze execution and AMLCO approval.