

KNOW YOUR CUSTOMER (KYC) POLICY & OPERATIONAL MANUAL

ALTBETR EXCHANGE Licensed Operator

Document Title	KYC Policy & Operational Manual
Version	1.0
Effective Date	March 2026
Classification	CONFIDENTIAL – INTERNAL USE ONLY
Regulatory Authority	Curacao Gaming Authority (CGA)
Review Cycle	Annual (or upon regulatory change)

This document is prepared in compliance with the Curaçao Gaming Control Ordinance, CGA Master Licence conditions, and applicable AML/CFT obligations.

DOCUMENT CONTROL

Version History

Version	Date	Description of Change
1.0	March 2026	Initial release — full KYC Policy & Operational Manual

Approval & Sign-Off

Role	Responsibility
MLRO / Compliance Officer	Responsible for drafting, maintaining, and enforcing this policy.
Chief Executive Officer	Approves this policy and ensures adequate resourcing.
Board of Directors	Ultimate accountability for AML/CFT compliance framework.

Document Distribution

This document is classified CONFIDENTIAL and is distributed on a need-to-know basis to:

- Compliance Department
- Customer Support / Onboarding Team
- Risk & Fraud Team
- Operations Management
- Senior Leadership / Board

TABLE OF CONTENTS

DOCUMENT CONTROL	2
Version History	2
Approval & Sign-Off	2
Document Distribution	2
TABLE OF CONTENTS	3
1. INTRODUCTION & PURPOSE	6
1.1 Background	6
1.2 Purpose	6
1.3 Policy Statement	6
1.4 Definitions	6
2. SCOPE & APPLICATION	8
2.1 Entities & Activities Covered	8
2.2 Restricted Jurisdictions	8
2.3 Relationship with Other Policies	8
3. REGULATORY FRAMEWORK	9
3.1 CGA Licensing Requirements	9
3.2 International Standards	9
3.3 Key Legislation & Guidance	9
4. RISK-BASED APPROACH	10
4.1 Overview	10
4.2 Business-Wide Risk Assessment	10
4.3 Customer Risk Rating	10
4.4 Risk Factors	10
Customer Risk Factors	10
Geographic Risk Factors	11
Product / Channel Risk Factors	11
5. CUSTOMER IDENTIFICATION PROGRAMME	12
5.1 General Principles	12
5.2 Minimum Information to be Collected	12
5.3 Identity Verification – Standard Documents	12
List A – Identity Documents (Primary)	12
List B – Proof of Address (Secondary)	12
5.4 Electronic / Automated Identity Verification (eIDV)	13
5.5 Age Verification	13
5.6 Corporate / Legal Entity Customers	13

6. CUSTOMER DUE DILIGENCE (CDD)	14
6.1 Standard CDD Requirements	14
6.2 Simplified Due Diligence (SDD)	14
6.3 CDD Timing	14
6.4 Inability to Complete CDD	14
7. ENHANCED DUE DILIGENCE (EDD)	16
7.1 When EDD is Required	16
7.2 EDD Measures	16
7.3 EDD for High-Risk Jurisdictions	16
7.4 Deposit / Wagering Thresholds Triggering EDD	17
8. POLITICALLY EXPOSED PERSONS (PEPs)	18
8.1 Definition of PEP	18
8.2 PEP Identification Process	18
8.3 Handling PEP Customers	18
9. SANCTIONS SCREENING	19
9.1 Sanctions Framework	19
9.2 Screening Obligations	19
9.3 Handling a Sanctions Match	19
9.4 No 'Tipping Off'	19
10. BENEFICIAL OWNERSHIP	21
10.1 Identification of UBOs	21
10.2 Documentation Requirements for UBOs	21
10.3 Complex Structures	21
11. SOURCE OF FUNDS & SOURCE OF WEALTH	22
11.1 Distinction	22
11.2 When SOF/SOW is Required	22
11.3 Acceptable SOF Documentation	22
11.4 Evaluation of SOF/SOW	22
12. ONGOING MONITORING	24
12.1 Principles	24
12.2 Periodic CDD Reviews	24
12.3 Trigger-Based Reviews	24
12.4 Customer Information Updates	24
13. TRANSACTION MONITORING	25
13.1 Overview	25
13.2 Monitoring Rules & Scenarios	25

13.3 Alert Investigation Process.....	25
13.4 Monetary Thresholds (Default – adjustable by MLRO).....	25
14. SUSPICIOUS ACTIVITY REPORTING (SAR)	27
14.1 Obligation to Report	27
14.2 Internal Reporting Process.....	27
14.3 External Reporting to FIU.....	27
14.4 Tipping-Off Prohibition	27
14.5 Record Keeping	27
15. RECORD KEEPING & DATA RETENTION	28
15.1 Retention Obligations.....	28
15.2 Storage & Security	28
15.3 Disposal	28
16. STAFF TRAINING & AWARENESS.....	29
16.1 Training Obligation	29
16.2 Training Content.....	29
16.3 Training Records.....	29
17. THIRD-PARTY RELIANCE.....	30
17.1 Use of Third Parties	30
17.2 Approved Third-Party Providers.....	30
17.3 Ongoing Oversight	30
18. ROLES & RESPONSIBILITIES	31
18.1 Money Laundering Reporting Officer (MLRO)	31
18.2 Compliance Department	31
18.3 All Employees	31
18.4 Board of Directors	31
19. POLICY REVIEW & UPDATES	32
19.1 Review Cycle	32
19.2 Communication of Changes.....	32
19.3 Escalation.....	32
APPENDICES.....	33
Appendix A – KYC Onboarding Checklist (Individual Customer).....	33
Appendix B – KYC Onboarding Checklist (Corporate Customer).....	34
Appendix C – Internal Suspicion Report (ISR) Template.....	35
Appendix D – Risk Rating Matrix	36
Appendix E – Glossary of Key Terms	37

1. INTRODUCTION & PURPOSE

1.1 Background

This Know Your Customer (KYC) Policy & Operational Manual (the "Policy") establishes the framework, procedures, and controls that [COMPANY NAME] (the "Company") applies to identify, verify, and understand its customers in compliance with the requirements of the Curaçao Gaming Authority (CGA) and applicable anti-money laundering (AML) and counter-terrorist financing (CTF) obligations.

The CGA issues and supervises licences under the national ordinance on offshore games of hazard ("Landsverordening buitengaats hazardspelen", P.B. 1993, no. 63) as amended, and requires all licensees to implement robust KYC and AML/CFT programmes.

1.2 Purpose

The primary purposes of this Policy are to:

- Prevent the Company's platforms and services from being used for money laundering, terrorist financing, or other financial crimes.
- Ensure full compliance with the CGA Licence conditions and all applicable AML/CFT laws, regulations, and guidelines.
- Establish clear, consistent, and risk-proportionate procedures for customer identification and due diligence.
- Protect the Company's reputation and the integrity of the gaming industry.
- Define roles, responsibilities, and escalation paths for KYC-related matters.

1.3 Policy Statement

The Company is committed to conducting business only with legitimate customers whose identity has been satisfactorily verified and whose source of funds is consistent with their profile. The Company will not knowingly provide services to individuals or entities involved in criminal activity, money laundering, terrorist financing, or sanctions violations.

1.4 Definitions

Abbreviation	Definition
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CGA	Curaçao Gaming Authority
CTF / CFT	Counter-Terrorist Financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer

Abbreviation	Definition
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
UBO	Ultimate Beneficial Owner

2. SCOPE & APPLICATION

2.1 Entities & Activities Covered

This Policy applies to:

- All online gaming and betting activities operated under the Company's CGA licence.
- All customer accounts, regardless of jurisdiction of the customer's residence (subject to restricted territories).
- All staff, contractors, agents, and third-party service providers acting on behalf of the Company.
- All payment channels, including but not limited to credit/debit cards, bank transfers, e-wallets, prepaid instruments, and cryptocurrency.

2.2 Restricted Jurisdictions

The Company does not accept customers from jurisdictions that:

- Are subject to FATF public statements (black or grey list countries).
- Are subject to UN, EU, US OFAC, or UK HMT comprehensive sanctions.
- Are explicitly prohibited under the CGA licence conditions.
- Have been internally designated as High-Risk Jurisdictions by the Company's Risk Committee.

The list of restricted jurisdictions is maintained by the Compliance Department and reviewed quarterly. Customers identified as residing in restricted jurisdictions will have their accounts blocked and funds returned through the original payment method.

2.3 Relationship with Other Policies

This Policy should be read in conjunction with:

- AML / CTF Policy
- Responsible Gaming Policy
- Data Protection & Privacy Policy (GDPR / local data protection laws)
- Sanctions Screening Policy
- Transaction Monitoring Policy
- Fraud Prevention Policy

3. REGULATORY FRAMEWORK

3.1 CGA Licensing Requirements

The Company holds a Master Gaming Licence issued by the Curaçao Gaming Authority. Under the CGA framework, licensees are required to:

- Implement a comprehensive KYC programme prior to activation of any customer account.
- Appoint a designated Money Laundering Reporting Officer (MLRO).
- Conduct customer due diligence proportionate to the risk presented by each customer.
- Maintain complete and accurate records of all KYC documentation for a minimum of five (5) years from the end of the business relationship.
- Report suspicious transactions to the Financial Intelligence Unit (FIU) of Curaçao.
- Cooperate fully with CGA examinations and requests for information.

3.2 International Standards

The Company's KYC framework is aligned with the FATF 40 Recommendations, in particular:

Recommendation	Application to the Company
FATF Rec. 10	Customer Due Diligence – financial institutions should be prohibited from keeping anonymous accounts.
FATF Rec. 11	Record Keeping – five-year retention requirement for CDD records and transaction data.
FATF Rec. 12	Politically Exposed Persons – enhanced measures for foreign PEPs, domestic PEPs, and international organisation PEPs.
FATF Rec. 15	New Technologies – risk assessment for new products and technology.
FATF Rec. 16	Wire Transfers – originator/beneficiary information for fund transfers.
FATF Rec. 19	Higher-Risk Countries – enhanced due diligence for customers from FATF high-risk jurisdictions.
FATF Rec. 20	Reporting of Suspicious Transactions – filing STR/SAR with FIU.

3.3 Key Legislation & Guidance

- National Ordinance on the Identification of Clients when Rendering Services (P.B. 1996, no. 23) – Curaçao
- National Ordinance on the Reporting of Unusual Transactions (P.B. 1996, no. 21) – Curaçao
- CGA Technical Standards and Compliance Guidelines (most recent version)
- FATF Guidance on the Risk-Based Approach for the Gambling Sector (2021)
- EGBA / Remote Gambling Sector AML/CFT Guidelines (reference only)

4. RISK-BASED APPROACH

4.1 Overview

The Company adopts a risk-based approach (RBA) to KYC. The depth and intensity of due diligence measures applied to each customer is proportionate to the assessed level of money laundering / terrorist financing (ML/TF) risk that the customer presents. This ensures that resources are targeted where they are most needed.

4.2 Business-Wide Risk Assessment

The Company conducts and documents a Business-Wide Risk Assessment (BWRA) at least annually. The BWRA considers:

- Products and services offered (e.g., sports betting, casino, live dealer, virtual sports).
- Customer base demographics and geographic spread.
- Delivery channels and payment methods.
- Emerging risks (new technologies, cryptocurrency, regulatory changes).

The BWRA is approved by the Board and forms the foundation for the customer risk-rating model.

4.3 Customer Risk Rating

Every customer is assigned a risk rating upon account opening and re-evaluated on an ongoing basis. The risk rating determines the level of due diligence applied.

Risk Level	Indicators	Due Diligence Level
LOW	Low-risk jurisdiction; verified identity; consistent low-volume activity; no adverse media or PEP/sanctions matches.	Standard CDD (SDD where applicable)
MEDIUM	Some elevated indicators present but no specific red flags; moderate transaction volumes; unfamiliar payment methods.	Standard CDD with periodic review
HIGH	High-risk jurisdiction; PEP status; unusual transaction patterns; high-value deposits; adverse media hits; multiple failed verification attempts.	Enhanced Due Diligence (EDD)

4.4 Risk Factors

Customer Risk Factors

- Residence or nationality in a high-risk jurisdiction
- PEP status (domestic, foreign, or international organisation)
- Adverse media or criminal record
- Complex ownership structures
- Inconsistency between stated income and actual betting/deposit behaviour
- Multiple failed identity verification attempts

Geographic Risk Factors

- Countries on FATF high-risk or under increased monitoring lists
- Countries subject to UN/EU/OFAC sanctions
- Countries with high levels of corruption (Transparency International CPI score below 40)
- Offshore financial centres with weak AML/CFT frameworks

Product / Channel Risk Factors

- High-velocity in-play betting
- Cryptocurrency deposits and withdrawals
- Third-party or non-personalised payment methods
- Multi-account activity
- Large single deposits or rapid accumulation of deposits

5. CUSTOMER IDENTIFICATION PROGRAMME

5.1 General Principles

The Company will not open, activate, or maintain any customer account without completing satisfactory identity verification. The KYC process is initiated at account registration and must be completed before a customer is permitted to:

- Make any deposit or payment.
- Place any wager or bet.
- Request any withdrawal.

Where KYC cannot be completed (e.g., customer fails to provide documents, documents are rejected), the account must be suspended and any funds held pending resolution or returned to source.

5.2 Minimum Information to be Collected

The following information must be collected from all individual customers:

Data Field	Purpose
Full Legal Name	As it appears on official government-issued identification.
Date of Birth	To confirm legal age (18+) and as identity verification element.
Country of Residence	Primary residential address (full address including postcode/ZIP).
Nationality	As stated on identity document.
Email Address	Primary contact and communication channel.
Mobile Phone Number	For two-factor authentication and communication.
Username / Account ID	Unique identifier within the Company's platform.

5.3 Identity Verification – Standard Documents

At least ONE primary document from List A, and ONE secondary document from List B must be provided to verify identity and address:

List A – Identity Documents (Primary)

- Valid national passport (any country)
- National identity card (government-issued, with photo)
- Valid driving licence (with photograph, issued by a recognised authority)

List B – Proof of Address (Secondary)

- Utility bill (gas, electricity, water) – not older than 3 months
- Bank or credit card statement – not older than 3 months
- Official government correspondence – not older than 6 months
- Tax authority correspondence – not older than 6 months

- Tenancy agreement (signed, with start date within 12 months)

Documents must be:

1. Legible and unaltered.
2. In a supported language (or accompanied by a certified translation).
3. Current and valid (not expired, unless otherwise specified above).
4. Submitted in colour; black-and-white copies are not acceptable.
5. Free from obstruction – all four corners and security features must be visible.

5.4 Electronic / Automated Identity Verification (eIDV)

The Company may utilise approved third-party electronic identity verification (eIDV) providers to perform automated identity checks. Such checks may include:

- Database checks (credit bureaus, electoral roll, mortality register).
- Document authentication (liveness checks, OCR, NFC chip reading).
- Biometric verification (facial recognition / selfie match).

eIDV checks must meet or exceed the standards of documentary verification. The Company retains records of all eIDV checks and outcomes.

5.5 Age Verification

Age verification is mandatory for all customers. The Company must confirm that the customer is at least 18 years of age (or the applicable legal gambling age in their jurisdiction of residence, whichever is higher) before any gaming activity is permitted.

If age cannot be confirmed, the account must be blocked immediately and any funds returned.

5.6 Corporate / Legal Entity Customers

Where a corporate or legal entity customer is accepted, the following additional information must be obtained:

- Full legal name and registered number of the entity.
- Registered address and principal place of business.
- Certificate of incorporation or equivalent formation document.
- Memorandum and Articles of Association (or equivalent).
- List of directors and senior management.
- Ownership structure chart identifying all shareholders with $\geq 10\%$ interest.
- Identification and verification of all Ultimate Beneficial Owners (UBOs) holding $\geq 25\%$ (or the applicable legal threshold).
- Authorisation for the individual acting on behalf of the entity.

6. CUSTOMER DUE DILIGENCE (CDD)

6.1 Standard CDD Requirements

Standard Customer Due Diligence (CDD) applies to all customers not otherwise qualifying for simplified treatment and not identified as high risk. Standard CDD consists of:

6. Identity verification (Section 5).
7. Verification of address.
8. Understanding the nature and purpose of the business relationship (gaming/betting).
9. Ongoing monitoring proportionate to the risk level (Section 12).

6.2 Simplified Due Diligence (SDD)

Simplified Due Diligence may be applied where the ML/TF risk associated with a customer is demonstrably low. SDD allows for reduced documentation requirements but does not eliminate CDD entirely. SDD may be considered for:

- Customers who are low-risk residents of EEA/EU member states with fully regulated gambling markets.
- Customers with long-standing verified accounts and consistent, low-risk behaviour.

Even where SDD is applied, the Company must still collect and verify the customer's full name and date of birth, and must escalate to Standard or Enhanced CDD if any red flags emerge.

6.3 CDD Timing

CDD must be completed:

Scenario	Timing Requirement
New Customers	Prior to account activation and before any deposit, wager, or withdrawal is permitted.
Existing Customers (periodic review)	At intervals defined by risk rating: High-risk annually; Medium-risk every 2 years; Low-risk every 3 years.
Existing Customers (trigger-based)	Upon occurrence of a trigger event (see Section 12.3).
Returning Customers (dormant accounts)	Before reactivation if inactive for more than 12 months.

6.4 Inability to Complete CDD

If the Company is unable to complete CDD to its satisfaction (including because a customer fails or refuses to provide required documentation), the Company must:

10. Suspend the customer account immediately.
11. Decline to process any pending transaction.
12. Return any funds held in the account to the original payment source.
13. Consider whether the circumstances are suspicious and, if so, file a Suspicious Activity Report (SAR) with the FIU.

14. Not 'tip off' the customer that an SAR has been or is being made.

7. ENHANCED DUE DILIGENCE (EDD)

7.1 When EDD is Required

Enhanced Due Diligence (EDD) is mandatory where a customer or transaction presents a higher risk of money laundering or terrorist financing. EDD is triggered in the following circumstances:

- The customer is identified as a Politically Exposed Person (PEP) or a close associate / family member of a PEP.
- The customer is resident in, or the source of funds originates from, a high-risk or sanctioned jurisdiction.
- The customer's cumulative deposits or wagers exceed defined thresholds (see 7.4).
- The customer's activity is inconsistent with their stated profile.
- There are adverse media findings or suspicious transaction patterns.
- The customer has been referred for EDD by the transaction monitoring system.
- At the MLRO's discretion based on judgment or intelligence.

7.2 EDD Measures

EDD involves the application of additional measures, which may include one or more of the following:

EDD Measure	Description
Enhanced Identity Verification	Additional identity document, biometric check, or independent database verification.
Source of Funds (SOF)	Documentary evidence of how the customer obtained the funds used for gaming (e.g., payslips, bank statements, business accounts, sale proceeds).
Source of Wealth (SOW)	Evidence of the customer's overall wealth and assets (e.g., tax returns, investment statements, property deeds).
Proof of Income	Recent payslips, employer letter, accountant's letter, or tax assessment.
Enhanced Ongoing Monitoring	Increased frequency of transaction reviews; lower thresholds for escalation.
Senior Management Approval	Approval from MLRO or senior management before establishing or continuing the relationship.
Adverse Media / Open-Source Checks	Structured searches of negative news, court records, and regulatory databases.
Network Analysis	Review of linked accounts, shared devices, or payment methods.

7.3 EDD for High-Risk Jurisdictions

Customers from FATF high-risk or under increased monitoring countries require EDD as a minimum, regardless of other risk factors. The Company applies the following specific measures for such customers:

- Full Source of Funds and Source of Wealth verification.
- MLRO approval required before account activation.
- Quarterly review of account activity.
- Enhanced transaction monitoring limits (50% of standard thresholds).

7.4 Deposit / Wagering Thresholds Triggering EDD

The following thresholds trigger mandatory EDD review:

Threshold	Required Action
Single deposit ≥ EUR 2,000 (or equivalent)	SOF documentation required; MLRO notified.
Cumulative deposits ≥ EUR 5,000 in rolling 30 days	Full KYC review; SOF and SOW required.
Cumulative deposits ≥ EUR 10,000 in rolling 90 days	Full EDD including SOW; Senior Management approval.
Net losses ≥ EUR 5,000 in rolling 30 days	SOF and SOW review; Responsible Gaming check.
Withdrawal request ≥ EUR 5,000 in rolling 7 days	Full CDD confirmation; SOF verification.

The MLRO may adjust the above thresholds at any time based on updated risk assessment. All changes must be documented.

8. POLITICALLY EXPOSED PERSONS (PEPs)

8.1 Definition of PEP

A Politically Exposed Person (PEP) is an individual who is, or has been, entrusted with a prominent public function. PEP categories include:

Category	Description
Foreign PEPs	Heads of state/government, senior politicians, senior government officials, senior judicial/military officials, senior executives of state-owned corporations, senior officials of political parties – in a foreign country.
Domestic PEPs	Individuals holding the above roles within Curaçao or the Kingdom of the Netherlands.
International Organisation PEPs	Senior management of international organisations (e.g., UN, IMF, World Bank, EU).
Close Associates	Individuals widely known to have close business or personal relationships with PEPs.
Family Members	Spouse/partner, children and their spouses/partners, parents of a PEP.

8.2 PEP Identification Process

All customers must be screened against PEP databases at account opening and on an ongoing basis. The Company uses an approved third-party screening provider that covers commercially available PEP lists. Screening must also be repeated:

- When a customer's information is updated.
- Periodically as part of the regular CDD review cycle.
- When a customer's risk rating changes.

8.3 Handling PEP Customers

When a customer is identified as a PEP or associated with a PEP, the following measures apply:

15. Senior Management Approval: MLRO or designated senior management must approve the onboarding or continuation of the relationship.
16. EDD: Full Enhanced Due Diligence must be applied, including SOF and SOW verification.
17. Ongoing Monitoring: The account is classified as High Risk and subject to enhanced ongoing monitoring.
18. Annual Review: The PEP relationship must be reviewed at least annually.

Former PEPs: An individual who has ceased to hold a prominent public function should continue to be treated as a PEP for a minimum period of 12 months (or longer at the MLRO's discretion) until the MLRO is satisfied that there is no longer an elevated risk.

9. SANCTIONS SCREENING

9.1 Sanctions Framework

The Company is required to comply with applicable international sanctions regimes. This includes, but is not limited to:

- United Nations Security Council (UNSC) consolidated sanctions list.
- European Union (EU) consolidated sanctions list.
- US Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list.
- UK His Majesty's Treasury (HMT) Financial Sanctions list.
- Any other sanctions list designated as applicable by the CGA or the Company's Risk Committee.

9.2 Screening Obligations

The Company must screen all customers against the applicable sanctions lists:

When	Obligation
At Onboarding	Before account activation. A match must prevent the account from being opened.
Ongoing	Daily screening against updated sanctions lists using an approved automated system.
On Name/Data Change	Whenever a customer updates their personal information.
Upon List Update	When a new name is added to a relevant sanctions list, all existing customers must be re-screened.

9.3 Handling a Sanctions Match

In the event of a positive or potential sanctions match:

19. Immediately freeze the account and suspend all transactions.
20. Escalate to the MLRO within 24 hours.
21. The MLRO investigates the match (true match vs. false positive).
22. If confirmed as a true match: report to the FIU / relevant authority; do not tip off the customer; block funds pending instructions from authorities.
23. If confirmed as a false positive: document the basis for the determination and re-activate the account.
24. All screening results, investigations, and determinations must be fully documented and retained for at least 5 years.

9.4 No 'Tipping Off'

At no point may any employee inform a customer or any third party that a sanctions check has been conducted, that a match has been identified, or that a report has been made to the FIU or any authority. Any breach of the tipping-off prohibition may constitute a criminal offence.

10. BENEFICIAL OWNERSHIP

10.1 Identification of UBOs

Where the Company onboards a corporate, legal entity, or trust customer, it must identify and verify the Ultimate Beneficial Owner(s) (UBOs). A UBO is any natural person who ultimately owns or controls the customer entity, or on whose behalf a transaction is being conducted.

The ownership threshold for identification is any natural person holding (directly or indirectly) 25% or more of the shares, voting rights, or ownership interest, or who exercises control by other means.

10.2 Documentation Requirements for UBOs

- Full legal name and date of birth of each UBO.
- Country of nationality and country of residence.
- Nature and extent of the beneficial interest held.
- Government-issued photo ID for each UBO (as per Section 5.3).
- Proof of address for each UBO.
- Where UBO holds through another entity: full ownership structure chart, certified by a director or legal representative.

10.3 Complex Structures

Where the ownership or control structure is complex or opaque (e.g., multi-layer holding companies, nominee shareholders, bearer shares), the Company must:

- Obtain a detailed group structure chart.
- Verify each intermediate layer.
- Apply EDD to all identified UBOs.
- Obtain MLRO approval before proceeding.

If the Company is unable to identify the UBO(s) with reasonable certainty, it must decline to establish or continue the business relationship.

11. SOURCE OF FUNDS & SOURCE OF WEALTH

11.1 Distinction

Concept	Definition
Source of Funds (SOF)	The origin of the specific funds being used for gambling/betting activities. Answers the question: "Where did this money come from?"
Source of Wealth (SOW)	The origin of the customer's entire wealth and assets. Answers the question: "How did this customer accumulate their overall wealth?"

11.2 When SOF/SOW is Required

SOF documentation is required when any deposit threshold in Section 7.4 is reached, or at the MLRO's discretion. SOW is required for High-Risk customers and EDD cases.

11.3 Acceptable SOF Documentation

Source Type	Acceptable Documentation
Employment Income	Recent payslips (last 3 months); employer confirmation letter; employment contract.
Self-Employment / Business	Recent business bank statements (last 6 months); audited accounts; accountant's letter.
Investment Returns	Brokerage statements; investment account statements; dividend payment notices.
Property / Asset Sale	Completion statements; sale agreements; land registry documents.
Inheritance / Gift	Solicitor letter; grant of probate; deed of gift.
Pension / Benefits	Pension statement; benefit award letter.
Winnings (Gaming / Lottery)	Documented proof of winnings from licensed operator.

11.4 Evaluation of SOF/SOW

The MLRO or designated compliance officer must evaluate SOF/SOW documentation and determine whether:

- The documentation is genuine and consistent with the customer's profile.
- The level of funds is consistent with the customer's declared income/wealth.
- The frequency and size of deposits is explainable.

If SOF/SOW cannot be adequately verified, the account must be suspended and an SAR considered.

12. ONGOING MONITORING

12.1 Principles

KYC is not a one-time event. The Company must conduct ongoing monitoring of all customer relationships to ensure that:

- The customer's profile and documentation remain up to date and accurate.
- The customer's transactions are consistent with the Company's knowledge of their profile, risk, and source of funds.
- Any changes in risk classification are identified and acted upon promptly.

12.2 Periodic CDD Reviews

Risk Level	Review Frequency
High Risk	At least once every 12 months.
Medium Risk	At least once every 24 months.
Low Risk	At least once every 36 months.

12.3 Trigger-Based Reviews

In addition to periodic reviews, an immediate CDD review is triggered by:

- Any transaction above the EDD thresholds (Section 7.4).
- A deposit or withdrawal pattern inconsistent with prior activity.
- Customer notification of change of address, employment, or financial status.
- Receipt of adverse information (media, law enforcement, third-party).
- A hit on PEP or sanctions screening.
- Suspicion of money laundering, terrorist financing, or fraud.
- A significant change in the customer's deposit or betting behaviour.

12.4 Customer Information Updates

Customers must be prompted to confirm or update their information at least every 12 months for High Risk accounts and every 24 months for Medium/Low risk accounts. The Company may request updated documentation at any time.

13. TRANSACTION MONITORING

13.1 Overview

The Company operates a transaction monitoring programme to detect unusual or suspicious activity. Transaction monitoring is conducted through a combination of automated rule-based systems and manual review.

13.2 Monitoring Rules & Scenarios

The following scenarios are among those monitored by the system:

- Large single deposits or withdrawals above defined thresholds.
- Multiple small deposits in rapid succession (structuring / smurfing indicators).
- Deposits immediately withdrawn without significant gaming activity.
- Unusual or inconsistent betting patterns (e.g., placing bets on both sides of an outcome).
- High frequency of transactions from the same IP address, device, or payment method.
- Deposits using multiple different payment methods within a short period.
- Requests to withdraw to a different payment method than used for deposit.
- Deposits inconsistent with stated income or financial profile.
- Activity following a dormancy period.

13.3 Alert Investigation Process

Stage	Action
Alert Generated	Automated system or manual analyst identifies a potential suspicious activity.
Level 1 Review	Compliance Analyst reviews the alert within 48 hours. Initial determination: escalate or dismiss.
Level 2 Review	Senior Compliance Officer reviews escalated alerts within 5 business days. Gathers additional evidence; interviews customer if appropriate.
MLRO Determination	MLRO makes final determination: no further action, enhanced monitoring, account restriction, or SAR filing.
Documentation	All alerts, reviews, and outcomes are documented and retained.

13.4 Monetary Thresholds (Default – adjustable by MLRO)

Scenario	Threshold
Single Deposit	≥ EUR 2,000 – triggers review.
Cumulative Deposits (30-day rolling)	≥ EUR 5,000 – triggers review.

Scenario	Threshold
Single Withdrawal	≥ EUR 3,000 – triggers review.
Net Deposits (90-day rolling)	≥ EUR 10,000 – mandatory EDD.
Structuring Pattern	3+ deposits < EUR 1,000 within 24 hours – review.

14. SUSPICIOUS ACTIVITY REPORTING (SAR)

14.1 Obligation to Report

All staff have a legal obligation to report knowledge or suspicion of money laundering or terrorist financing to the MLRO promptly. The MLRO is responsible for evaluating internal reports and, where appropriate, filing a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) of Curaçao ("Meldpunt Ongebruikelijke Transacties", MOT).

14.2 Internal Reporting Process

25. Any employee who suspects that a transaction or activity may involve money laundering or terrorist financing must complete an Internal Suspicion Report (ISR) and submit it to the MLRO immediately, and in any case within 24 hours.
26. The ISR must include: the customer's details; the nature of the transaction; the basis for suspicion; any supporting documentation.
27. The MLRO must acknowledge receipt of the ISR within 24 hours.
28. The MLRO reviews the ISR and makes a determination within 5 business days (sooner where time-sensitive).

14.3 External Reporting to FIU

Where the MLRO determines that there are reasonable grounds to suspect money laundering or terrorist financing, the Company must file an STR/SAR with the FIU. STRs must be filed:

- Within the timeframe prescribed by applicable law (typically within 24 hours of forming the suspicion for high-risk cases).
- Using the FIU's prescribed reporting format.
- Containing all required information about the transaction, the customer, and the grounds for suspicion.

14.4 Tipping-Off Prohibition

It is a criminal offence to disclose ("tip off") to the customer or any other person that a suspicion has been formed, that an ISR or SAR has been filed, or that an investigation is being conducted. This prohibition applies to all employees and must be communicated during staff training.

14.5 Record Keeping

All ISRs, MLRO determinations, SARs filed, and supporting materials must be retained for a minimum of 5 years and must be available for inspection by the CGA, FIU, or other competent authority.

15. RECORD KEEPING & DATA RETENTION

15.1 Retention Obligations

The Company must retain the following records for a minimum of five (5) years from the end of the business relationship or the date of the transaction, whichever is later:

Record Type	Description
KYC / CDD Documents	Copies of identity documents, proof of address, SOF/SOW documentation, eIDV reports, and all CDD records.
Account Records	Customer account data, registration information, and all changes to customer information.
Transaction Records	Full record of all financial transactions, including deposits, withdrawals, bets, and winnings.
Correspondence	Customer communications relevant to KYC, compliance, or suspicious activity.
SAR / ISR Records	All internal suspicion reports, MLRO decisions, and SARs filed with the FIU.
Screening Records	PEP and sanctions screening results, including false positives and true match investigations.
Training Records	Records of staff training completion, dates, and assessments.

15.2 Storage & Security

- All records must be stored securely, with access restricted to authorised personnel.
- Electronic records must be stored in a system that prevents unauthorised alteration and ensures auditability.
- Records must be readily retrievable and available to the CGA, FIU, or other competent authority upon request.
- The Company must comply with all applicable data protection laws (including the Curaçao Personal Data Protection Ordinance and, where applicable, EU GDPR) when storing and processing personal data.

15.3 Disposal

Upon expiry of the retention period, records may be securely destroyed provided there is no ongoing investigation, legal proceeding, or regulatory inquiry that requires their retention. Destruction must be logged.

16. STAFF TRAINING & AWARENESS

16.1 Training Obligation

All employees whose role involves customer onboarding, payments, compliance, risk, or management must receive adequate and regular AML/CFT and KYC training. Training must be:

- Conducted at induction before any employee undertakes KYC or compliance-related duties.
- Refreshed at least annually, or more frequently if there are material regulatory changes.
- Role-specific, with enhanced training for compliance and MLRO staff.

16.2 Training Content

Training programmes must cover:

- The Company's KYC Policy and operational procedures.
- The legal and regulatory framework applicable to the Company.
- How to identify and handle suspicious activity.
- The internal reporting process (ISR to MLRO).
- Tipping-off prohibition and its consequences.
- PEP and sanctions screening obligations.
- Record-keeping requirements.
- Consequences of non-compliance (disciplinary action and criminal liability).

16.3 Training Records

The Compliance Department must maintain records of all training completed, including the employee's name, date of completion, training content/version, and assessment results (if applicable). These records must be available for inspection by the CGA.

17. THIRD-PARTY RELIANCE

17.1 Use of Third Parties

The Company may rely on third-party service providers (e.g., KYC technology vendors, payment processors, affiliate partners) to perform elements of the CDD process. Where reliance is placed on a third party:

- The Company must satisfy itself that the third party is subject to equivalent AML/CFT requirements and supervision.
- The Company remains fully responsible for the adequacy of the CDD conducted; responsibility cannot be outsourced.
- A formal written agreement (Data Processing Agreement / KYC Reliance Agreement) must be in place.
- The Company must be able to obtain from the third party, without delay, copies of all CDD documentation.

17.2 Approved Third-Party Providers

The Compliance Department maintains a register of approved KYC and screening service providers. Any new third-party engagement for KYC/AML services must be approved by the MLRO prior to onboarding.

17.3 Ongoing Oversight

Third-party providers are subject to annual due diligence review by the Compliance Department to ensure continued compliance with the Company's standards and applicable regulation.

18. ROLES & RESPONSIBILITIES

18.1 Money Laundering Reporting Officer (MLRO)

The MLRO is the central point of responsibility for AML/CFT compliance. Key responsibilities include:

- Oversight and implementation of this Policy.
- Receipt and evaluation of internal suspicion reports (ISRs).
- Filing SARs/STRs with the FIU where required.
- Liaison with the CGA, FIU, and other competent authorities.
- Reporting to senior management and the Board on AML/CFT matters.
- Maintaining and updating the Business-Wide Risk Assessment.
- Overseeing the training programme.

18.2 Compliance Department

- Day-to-day KYC operations and document review.
- Customer onboarding and verification.
- Transaction monitoring alert management.
- PEP and sanctions screening.
- Maintenance of KYC records.

18.3 All Employees

- Adherence to this Policy and all related procedures.
- Reporting suspicious activity to the MLRO without delay.
- Completing all required training.
- Not disclosing (tipping off) customers or third parties about KYC/SAR activities.

18.4 Board of Directors

- Ultimate accountability for the AML/CFT compliance framework.
- Approving this Policy and allocating adequate resources.
- Receiving regular updates on AML/CFT compliance status.

19. POLICY REVIEW & UPDATES

19.1 Review Cycle

This Policy is reviewed at least annually by the MLRO and approved by the Board or designated senior management. An interim review may be triggered at any time by:

- A material change in the regulatory environment (CGA guidance, FATF updates, etc.).
- A significant change in the Company's products, services, or customer base.
- Identification of material deficiencies in the existing framework.
- A significant AML/CFT incident or regulatory finding.

19.2 Communication of Changes

Material changes to this Policy must be communicated to all relevant staff promptly and incorporated into training materials. A new version number, effective date, and summary of changes must be recorded in the Document Control section.

19.3 Escalation

Any employee who believes this Policy is inadequate or is not being followed must escalate their concerns to the MLRO or, if the MLRO is involved in the matter, directly to senior management or the Board.

APPENDICES

Appendix A – KYC Onboarding Checklist (Individual Customer)

#	Task	Status
1	Full legal name collected	☐
2	Date of birth collected & age verified (18+)	☐
3	Country of residence and address collected	☐
4	Email address and phone number collected	☐
5	Primary ID document received and verified (List A)	☐
6	Proof of address received and verified (List B)	☐
7	eIDV check completed (if applicable)	☐
8	PEP screening completed – outcome documented	☐
9	Sanctions screening completed – outcome documented	☐
10	Risk rating assigned (Low / Medium / High)	☐
11	EDD initiated if High Risk (Section 7)	☐
12	SOF documentation obtained (if applicable)	☐
13	MLRO approval obtained (if required)	☐
14	Account activated / onboarding outcome recorded	☐

Appendix B – KYC Onboarding Checklist (Corporate Customer)

#	Task	Status
1	Entity name and registration number collected	☐
2	Registered address and principal place of business collected	☐
3	Certificate of Incorporation / formation document obtained	☐
4	Memorandum & Articles of Association obtained	☐
5	List of directors and senior management obtained	☐
6	Ownership structure chart obtained and verified	☐
7	All UBOs (≥25%) identified	☐
8	Individual KYC completed for each UBO	☐
9	PEP screening for directors and UBOs – outcome documented	☐
10	Sanctions screening for entity and principals – outcome documented	☐
11	Risk rating assigned	☐
12	EDD initiated if required	☐
13	MLRO approval obtained	☐
14	Account activated / onboarding outcome recorded	☐

Appendix C – Internal Suspicion Report (ISR) Template

Complete this form and submit to the MLRO immediately upon forming a suspicion.

Field	Detail
Reporting Employee Name	
Department / Role	
Date of Report	
Customer Account ID	
Customer Full Name	
Date of Suspicious Activity	
Description of Suspicious Activity	(Describe the nature of the transaction or behaviour that gave rise to suspicion. Include dates, amounts, payment methods, and any relevant context.)
Basis for Suspicion	(Explain why you believe the activity may constitute money laundering or terrorist financing.)
Supporting Documents Attached	Yes / No – List documents:
Has the customer been informed?	Yes / No (If Yes, explain – note: tipping off is prohibited)
MLRO Receipt Acknowledgement	Date / Signature:

Appendix D – Risk Rating Matrix

The following matrix provides guidance on risk scoring. The overall risk rating is determined by the weighted combination of scores across all relevant risk factors.

Risk Factor	Low (1)	High (3)
Jurisdiction of Residence	EEA / EU / Australia / Canada / NZ / UK	FATF grey/black list; sanctioned country
Nationality	Same as low-risk jurisdiction	High-risk or sanctioned country
PEP Status	No PEP link	PEP or close associate/family member
Adverse Media	No negative results	Credible negative news or criminal record
Deposit Behaviour	Consistent with profile; below thresholds	Exceeds EDD thresholds; inconsistent with profile
Payment Method	Own bank account; major card	Crypto; third-party payment; prepaid card
Account History	Long-standing, no issues	New account; prior flags or restrictions

Appendix E – Glossary of Key Terms

Term	Definition
Beneficial Owner	The natural person(s) who ultimately owns or controls a customer, or on whose behalf a transaction is being conducted.
Business-Wide Risk Assessment (BWRA)	A documented assessment of the ML/TF risks facing the Company as a whole.
CDD (Customer Due Diligence)	The process of identifying and verifying a customer's identity and understanding the nature of the business relationship.
EDD (Enhanced Due Diligence)	Heightened due diligence measures applied to higher-risk customers or situations.
eIDV	Electronic Identity Verification – automated systems used to verify customer identity using digital data sources.
FIU	Financial Intelligence Unit – the national authority responsible for receiving and analysing STR/SAR reports.
MLRO	Money Laundering Reporting Officer – the designated individual responsible for receiving internal suspicion reports and filing SARs with the FIU.
PEP (Politically Exposed Person)	An individual entrusted with a prominent public function, as defined in Section 8.1.
Risk-Based Approach (RBA)	An approach to AML/CFT compliance that focuses resources proportionate to the identified level of risk.
SAR / STR	Suspicious Activity Report / Suspicious Transaction Report – a report filed with the FIU when ML/TF is suspected.
SDD (Simplified Due Diligence)	Reduced CDD measures applicable where the risk of ML/TF is demonstrably low.
Source of Funds (SOF)	Evidence of the origin of funds used in a specific transaction or series of transactions.
Source of Wealth (SOW)	Evidence of how a customer accumulated their overall wealth.
Tipping Off	The criminal offence of disclosing to a customer or third party that a suspicion has been reported or an investigation is underway.
UBO (Ultimate Beneficial Owner)	See Beneficial Owner above.