

Identification and Verification (KYC) Policy

1. Purpose & Scope

This policy sets out the mandatory requirements for identifying and verifying players.

2. Regulatory Basis

This Policy implements the obligations on identification and verification of players, including:

- Collection of personal data sufficient to establish identity (identification); and
- Confirmation of those details using reliable, independent sources such as documents (verification), applying a risk-based approach (RBA).

Primary regulatory source (Curaçao):

- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction — Applicable to Curaçao casinos and providers of other online games, issued by the Gaming Control Board / Curaçao Gaming Authority (GCB/CGA).

3. Definitions

- Identification: Collection of personal details to establish a player's identity.
- Verification: Confirmation of the collected details via reliable, independent documents/ data.
- Reliable independent source: Government-issued records; regulated financial institutions; trusted utility providers; qualified digital identity providers
- Document standard : Minimum quality and authenticity criteria a document must meet to be accepted.

4. Player Identification

At account opening the following personal information is collected to identify the player:

- Full name and surname
- Residential address

- Date of birth

Additional data may be collected for High risk situations: place of birth, nationality, identity number

5. Player Verification

5.1 Documents Standards

Acceptable Documents

Purpose	Primary examples	Alternative examples	Validity / Recency
Photo ID	Passport; National ID card	Driving Licence (photo); Residence permit	Unexpired; photo clear; full page/front&back
Proof of Address (PoA)	Utility bill; Bank/credit statement;	Tenancy/lease agreement; Insurance letter; Government benefits letter; Tax letter	Issued ≤ 6 months
Proof of ownership of payment account used on our site	Bank statement or online banking page showing account holder name, , and recent transaction(s) with our merchant	Card copy (front & back) with PAN masked (first 6/last 4 only), name and expiry visible; e-wallet account page (e.g., Skrill/Neteller) showing registered name/email and/or recent transaction(s); Payment provider/bank confirmation letter	Issued ≤ 6 months (or covers the most recent deposit). CVV fully covered; signature strip visible; no third-party accounts

- **Quality Criteria:** unobstructed, full edges visible, no glare/blur, readable MRZ/ID number, consistent metadata (names, dates, address). Foreign documents require extra care and, where necessary, translation.
- **Rejection Reasons (non-exhaustive):** Cropped/blurred; expired; altered; mismatch with account data; third-party documents; screenshots of mobile banking without issuer; unverifiable providers; suspected forgery

Non-Documentary Verification Methods:

- Geolocation/IP/device fingerprint: Consistency checks vs. declared country/address.
- Registry/database checks: Electoral roll, credit reference data, company registries, telephone directories.
- Contact: Phone call or secure message to corroborate facts.
- Video: Where enabled, biometric face-match with liveness to confirm that the person presenting the ID is the same individual and physically present.
- Any other reliable methods that reasonably confirm the identity of the player

5.2 Verification Timing & Triggers

- Onboarding: Identification initiated at registration (collect personal details: name and surname, permanent residential address and date of birth);
- Complete identity verification before first withdrawal or upon risk trigger—whichever occurs first.
- Threshold trigger: Complete verification when engaging in financial transactions (deposits and/or withdrawals) equal to or in excess of NAf 4,000. All CDD measures must be completed no later than 30 calendar days from the moment the threshold is reached.
- Event-driven triggers / red flags (pre-threshold): If any ML/TF red flags arise before the threshold (e.g., unusual device/geo, third-party payment indicators, inconsistencies in identity data, tampered documentation; PEP/sanctions match; geo anomalies; fraud indicators, etc), apply CDD and, where appropriate EDD regardless of value.

5.3 Verification Outcomes & Actions

Outcome	Description	Account status / next steps
Verified	Documents/data meet documents acceptance standards; match to account; checks passed	Full access; standard monitoring
Partially Verified	Verified identity but other documents are incomplete or missing (e.g., PoA expired; payment ownership pending)	Access allowed; pending withdrawals; obtain missing items

Not Accepted	Failed consistency checks (expired/forged/altered; data mismatch); suspected forgery	May suspend or restrict; consider EDD/ SAR as appropriate; request additional information/ clarification
Unresponsive	No response or uploads after KYC request(s) within defined timeframe	Re-initiate; set final deadline; suspend or maintain restrictions per risk; consider account closure if persistent

Escalation: Any High-risk case or repeated failures is escalated to the CDD & AML Team and the MLRO for review.

6. Record-Keeping & Audit Trail:

- Store copies of KYC documents in the player's folder
- Retain for 5 years (or longer if required by law/regulator). Apply access controls.
- Maintain records of CDD on player's account: what was checked, by whom, exceptions and approvals.