

Know Your Customer (KYC) Policy

Zerone B. V.

Version 1.0

1. Introduction

This Know Your Customer (KYC) Policy outlines the identity verification procedures adopted by Zerone B. V. in compliance with the requirements of the Curaçao Gaming Authority (CGA) and international best practices for Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF).

All KYC verifications are performed manually by trained personnel, ensuring accuracy, security, and regulatory compliance. The company maintains a strict identity verification standard before allowing customers to perform financial operations.

2. Purpose

The objectives of this KYC Policy are to:

1. Ensure the true identity of all customers using the platform.
 2. Prevent unverified customers from initiating or completing withdrawal requests.
 3. Reduce risks related to fraud, financial crime, and misuse of the gaming platform.
 4. Maintain complete documentation and audit-ready records for regulatory inspections.
 5. Support transparent and responsible gaming operations.
-

3. Scope

This policy applies to:

- All customers registered with Zerone B. V.
- All withdrawal requests.
- Identity and residency verifications required before any withdrawal can be processed.
- All manual analysis performed by Compliance personnel under the responsibility of Zerone B. V..

Important:

Customers cannot initiate any withdrawal request unless their KYC verification is fully completed and approved.

The system automatically blocks all withdrawal attempts for non-verified accounts.

4. Customer Identification and Verification Process

KYC verification is performed manually, following strict guidelines and conducted exclusively by trained Analysts.

4.1 Mandatory Documents

Customers must provide the following documents:

A. Valid Identification Document containing CPF

Accepted documents:

- RG (Brazilian Identity Card)
- CNH (Brazilian Driver's License)
- Passport + CPF (Brazilian Taxpayer Identification Number)

Requirements:

- Must be valid.
- Must be legible and unaltered.
- Must include a clear photograph.
- CPF must be present (either on the ID or as a separate official document).

B. Proof of Address (issued within the last 6 months)

Accepted documents:

- Electricity bill
- Water bill
- Landline phone bill
- Internet bill
- Any official government-issued document containing the residential address

Requirements:

- Must display the customer's full name and address.
- Must be fully legible and authentic.
- Must not exceed 6 months of issuance.

5. Manual KYC Verification Procedure

The verification process includes the following steps:

5.1 Step 1 — Document Submission

- The customer uploads the required documents through the platform.
- The system performs basic file validation (no automated identity checks).

5.2 Step 2 — Manual Initial Review

A trained Analyst evaluates:

- Legibility of all documents
- Validity and expiration dates
- Data consistency across documents
- Match between account information and submitted documents
- Signs of tampering, manipulation, or forgery

5.3 Step 3 — Manual Identity Authentication

The analyst confirms:

- Full name
- Date of birth
- CPF number
- Residential address
- Match between the photo ID and the customer's profile information

5.4 Step 4 — Verification Outcome

Status	Conditions	Action
Approved	All documents valid and consistent	Customer is allowed to request withdrawals
Rejected (Resubmit Required)	Documents unreadable, invalid, not compliant, cut, illegible, or incomplete	Customer is notified and requested to resubmit valid documentation
Rejected (Escalated)	Fraudulent, altered, or inconsistent documents	Account is suspended and escalated to the Fraud & Risk Department for further investigation

6. Ongoing Monitoring & Risk Controls

Although KYC verification is conducted manually, ongoing monitoring is maintained to reduce the risk of fraud, account misuse, and money laundering.

6.1 Monitoring Indicators

The company monitors:

- Attempts to create multiple accounts
- Betting patterns inconsistent with customer profile
- Unusual or high-risk transactional behavior
- Attempts to bypass identity verification
- Frequent or unexplained changes in personal information

6.2 Mitigation Measures

If suspicious activity is detected, the company may:

- Request additional documentation
 - Temporarily suspend the account
 - Initiate a full internal investigation
 - Report the incident to the CGA, if required
 - Implement enhanced due diligence procedures (EDD)
-

7. Data Storage and Security (LGPD-Compliant)

The company ensures the secure handling of customer data and KYC documents as follows:

- All documents are stored on encrypted servers with secure access controls.
- Access to KYC documents is restricted to authorized personnel only, including Customer Support agents, administrators, Compliance, Fraud, Risk & Payments, and Internal Audit teams, based on their roles and responsibilities.
- All personnel with access are trained in data privacy, security protocols, and KYC procedures.
- Access is monitored and logged, ensuring traceability of who accessed the documents, when, and for what purpose.
- Customer records are maintained for a minimum of 5 years, following AML best practices.

- The company complies with Brazil's Lei Geral de Proteção de Dados (LGPD) and international data protection standards.

All information is treated as confidential and protected from unauthorized access.

8. Internal Roles and Responsibilities (revised)

Department / Team Responsibilities

Compliance / KYC Team	Performs manual analysis and verification of KYC documents; approves or rejects documents; oversees and reviews KYC processes to ensure compliance with internal policies and regulatory requirements.
Customer Support (CS)	Assists customers with submitting KYC documentation; may review documents as part of customer interaction.
Fraud, Risk & Payments Teams	May review KYC documents for fraud prevention, risk assessment, and payment verification purposes.
Platform Service Provider (Third-Party)	Responsible for maintaining platform security and implementing technical safeguards.

Notes:

- All personnel with access are trained in data privacy, KYC procedures, and security protocols.

9. Record Keeping & Audit Procedures

- All KYC checks are logged with timestamps, analyst identification, results, and document metadata.
- Records are securely archived and made available to the CGA upon request.
- Internal audits are performed periodically to assess procedural integrity and regulatory compliance.

10. Policy Review and Updates

This policy is reviewed:

- Annually, or
- Following regulatory updates issued by the CGA, or
- When operational changes require modifications.

All changes are documented with version history and approval records.