

Know Your Customer (KYC) Policy

Effective Date: 29/06/2025

Approved By: Nicola Lawrance

Last Review Date: 01/09/2025

Next Review Date: 01/02/2026

1. Purpose & Scope

1.1 The purpose of this KYC Policy is to ensure that **Geeker NV**:

- Verifies the identity of all customers.
- Mitigates the risk of money laundering, fraud, and terrorist financing.
- Complies with **Curaçao eGaming LOK license**, the **National Ordinance on Identification (LID)**, and **Reporting Unusual Transactions (LMOT)**.

1.2 This policy applies to:

- All customers of Geeker NV, including players registering online.
- Employees, agents, and affiliates responsible for customer onboarding, monitoring, and reporting.

2. Customer Identification Program (CIP)

2.1 Information Collection

During account registration, the following information must be collected and verified:

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

- Government-issued identification (passport, national ID, driver's license)
- Proof of address (utility bill, bank statement, or official correspondence within the last 3 months)
- Payment method details (bank card, e-wallet, cryptocurrency wallet)

2.2 Verification Procedures

- Identity documents must be validated using reliable, independent sources.
- Payment methods must be verified to ensure the owner matches the registered customer.
- Cryptocurrency payments must follow the same verification as fiat currencies, with additional checks for high-value or high-risk transactions.

3. Risk Assessment and Enhanced Due Diligence (EDD)

3.1 Risk Categorization

Customers are classified as **low**, **medium**, or **high risk** based on:

- Jurisdiction of residence
- Transaction volume and frequency
- Source of funds
- Type of games and betting patterns

3.2 High-Risk Customers

EDD is required for:

- Politically Exposed Persons (PEPs)
- Customers from high-risk jurisdictions
- Customers with large or unusual transactions
- Cryptocurrency users with significant transfers

3.3 EDD Measures

Enhanced due diligence includes:

- Collecting additional documentation
 - Conducting background checks
 - Monitoring ongoing transactions more intensively
-

4. Ongoing Monitoring

- Continuous monitoring of customer transactions to detect unusual or suspicious activities.
 - Automated and manual systems track deviations from normal behavior patterns.
 - High-risk customers receive enhanced scrutiny and reporting.
-

5. Reporting Suspicious Activity

- Employees must immediately report any suspicious activity to the **Compliance Officer**.
 - The Compliance Officer will evaluate and, if necessary, file reports with the **Curaçao Financial Intelligence Unit (FIU)**.
-

6. Record Keeping

- All KYC documentation and verification results must be retained for a minimum of **5 years** after account closure.
 - Records include: identification documents, proof of address, payment verification, risk assessments, and transaction history.
-

7. Employee Training

- All staff involved in customer onboarding and monitoring receive mandatory KYC and AML training.
- Training is updated regularly to reflect regulatory changes and internal procedural updates.

8. Compliance Officer

- A designated Compliance Officer is responsible for ensuring adherence to KYC, AML, and LOK regulations.
 - Responsibilities include reviewing high-risk accounts, reporting suspicious transactions, and updating internal procedures.
-

9. Data Protection

- Customer data is stored and processed in compliance with applicable **data protection laws**.
 - Access to sensitive information is limited to authorized personnel only.
-

10. Review and Updates

- This KYC Policy is reviewed **annually** when significant changes occur in regulations or business operations.
- Updates require approval from senior management and are communicated to all relevant staff.