

1. Purpose & Scope

This KYC Policy (“the Policy”) establishes the standards and procedures Gleneagles B.V. applies to identify and verify customers, assess and monitor risk, and prevent the use of its gaming services for money-laundering, terrorist financing, or other financial crime.

It fulfils the requirements of the Curaçao Gaming Authority (CGA) and relevant AML/CFT legislation under the National Ordinance on Games of Chance (LOK).

This Policy applies to all customer relationships, both new and existing, and any account or transaction requiring enhanced review.

2. Risk-Based Approach

Gleneagles B.V. adopts a risk-based approach to Customer Due Diligence (CDD). The level of verification applied is proportionate to the risk presented by each customer. Key risk factors include:

- **Geographic risk** – residency or activity in high-risk jurisdictions.
- **Payment methods** – use of anonymous or high-risk channels.
- **Transaction behaviour** – large, rapid or inconsistent flows.
- **Customer profile** – PEP status, complex ownership, unknown funds source.

A documented risk-scoring model assigns each customer a rating (low/medium/high), reviewed periodically or on trigger events.

3. Customer Identification and Verification

3.1 Standard Due Diligence (SDD)

Before activation of a real-money account, Gleneagles B.V. must:

Identity Verification

- Obtain government-issued photo ID (passport, ID card or driver's licence).
- Verify name, date of birth and nationality.
- Confirm minimum legal age (18+).
- Validate document authenticity through independent means.

Payment Method Verification

- Confirm ownership of all payment instruments.
 - Ensure bank and account names match customer records.
-

4. Ongoing Monitoring

Continuous monitoring includes:

- Reviewing transaction patterns for suspicious behaviour.
 - Re-verifying identity on material profile changes.
 - Periodic risk reviews at least annually for high-risk customers.
 - Automated alerts for threshold breaches or unusual velocity.
-

5. Record-Keeping and Retention

All KYC and transaction records are kept for **a minimum of five (5) years** after account closure.

Records include identity documents, verification logs, risk scores, SARs, and EDD decisions.

Data is stored securely with restricted access and encryption.

6. Suspicious Activity Reporting

Where suspected money-laundering or terrorist financing is identified:

1. File a **Suspicious Activity Report (SAR)** with the Financial Intelligence Unit (FIU Curaçao).
 2. Prohibit "tipping-off" the customer.
 3. Maintain internal records of all SARs and supporting analysis.
 4. Notify the Compliance Officer and senior management.
-

7. Sanctions and PEP Controls

Screening occurs at onboarding and regular intervals (quarterly minimum). Positive matches are subject to EDD and senior-level approval before continuation or account closure.

8. Employee Training and Awareness

All staff involved in customer-facing or payment processes receive annual training on KYC, AML/CFT and Responsible Gaming. Training completion is recorded and audited by the Compliance Officer.

9. Oversight and Audit

- The Compliance Officer reviews this Policy at least annually.
 - Internal audit testing verifies control effectiveness and recommends improvements.
 - Updates are submitted to the Board for approval and implementation.
-

10. Enforcement and Customer Sanctions

Failure to complete KYC results in account restriction or closure. Employees who breach this Policy face disciplinary action up to termination.

11. Data Protection and Confidentiality

All KYC data is processed in accordance with GDPR and local data-protection laws. Information is restricted to authorised personnel and used solely for compliance purposes. Third-party processors are subject to binding data protection agreements.
