
*KNOW YOUR CUSTOMER (KYC) AND
CUSTOMER DUE DILIGENCE (CDD) POLICY*

KING ENTERPRISES N.V.

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

POLICY OWNER: KING ENTERPRISES N.V.

APPROVER: VASIL TONCHEV

DATE APPROVED: MAY 10, 2026

REVIEW FREQUENCY: ANNUALLY

NEXT REVIEW DATE: MAY 10, 2027

SECURITY CLASSIFICATION: CONFIDENTIAL

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

TABLE OF CONTENTS

1. Purpose	4
2. Scope	4
3. Definitions	5
3.1 Know Your Customer (KYC)	5
3.2 Customer Due Diligence (CDD)	5
3.3 Enhanced Due Diligence (EDD)	5
3.4 Politically Exposed Person (PEP)	5
3.5 Beneficial Owner.....	5
3.6 Suspicious Activity.....	5
4. Roles and Responsibilities	5
4.1 Compliance Department	5
4.2 Customer Service and Operations Teams	6
4.3 Fraud and Risk Teams	6
4.4 Management	6
5. Customer Identification Requirements	6
6. Identity Verification Procedures.....	7
7. Risk-Based Customer Due Diligence	8
8. Enhanced Due Diligence (EDD).....	9
8.1 Situations Requiring EDD	9
8.2 Additional EDD Measures.....	10
9. Ongoing Monitoring.....	10
10. Sanctions and PEP Screening.....	10
11. Source of Funds and Source of Wealth	12
12. Suspicious Activity Reporting and Escalation	12
13. Record Retention	13
14. Data Protection and Confidentiality.....	13
15. Training and Awareness	14
16. Non-Compliance	14
16.1 Player Non-Compliance	14
16.2 Employee Non-Compliance	15
17. Policy Review and Updates	15
Appendix A – Examples of Acceptable Documents	17
Appendix B – Examples of Red Flags	18
Appendix C – Escalation Workflow	19

1. PURPOSE

The purpose of this Know Your Customer (KYC) and Customer Due Diligence (CDD) Policy is to establish a framework for identifying, verifying, monitoring, and managing player relationships in order to:

- Prevent money laundering, terrorist financing, fraud, identity theft, and other financial crimes.
- Ensure compliance with applicable laws, regulations, and licensing requirements.
- Protect the integrity, reputation, and security of the company.
- Promote a risk-based approach to customer onboarding and monitoring.

This policy applies to all employees, contractors, agents, and third-party service providers involved in player onboarding, account management, payments, compliance, fraud prevention, and customer support.

2. SCOPE

This policy applies to:

- All players registering or maintaining accounts with the company.
- All payment methods, deposits, withdrawals, transfers, and related transactions.
- All jurisdictions in which the company operates.
- All business units and departments responsible for player interactions and account management.

This policy covers:

- Customer Identification Program (CIP).
- Identity Verification.
- Customer Due Diligence (CDD).
- Enhanced Due Diligence (EDD).
- Ongoing Monitoring.
- Record Retention.
- Suspicious Activity Escalation.
- Sanctions and Politically Exposed Person (PEP) Screening.

3. DEFINITIONS

3.1 KNOW YOUR CUSTOMER (KYC)

KYC refers to the process of verifying the identity of players and assessing their suitability and risk profile before and during the business relationship.

3.2 CUSTOMER DUE DILIGENCE (CDD)

CDD refers to the procedures used to gather and evaluate player information to understand the nature of the player relationship and assess potential risks.

3.3 ENHANCED DUE DILIGENCE (EDD)

EDD refers to additional verification and monitoring procedures applied to high-risk players or situations.

3.4 POLITICALLY EXPOSED PERSON (PEP)

A PEP is an individual who holds or has held a prominent public position, including close associates and immediate family members.

3.5 BENEFICIAL OWNER

A beneficial owner is the individual who ultimately owns or controls an account, entity, or transaction.

3.6 SUSPICIOUS ACTIVITY

Any activity that appears unusual, inconsistent with expected behavior, or potentially related to financial crime, fraud, money laundering, or sanctions violations.

4. ROLES AND RESPONSIBILITIES

4.1 COMPLIANCE DEPARTMENT

The Compliance Department is responsible for:

- Maintaining and updating this policy.

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

- Ensuring regulatory compliance.
- Reviewing escalated cases.
- Conducting enhanced due diligence reviews.
- Filing suspicious activity reports where required.
- Delivering compliance training.

4.2 CUSTOMER SERVICE AND OPERATIONS TEAMS

Customer Service and Operations personnel are responsible for:

- Collecting and reviewing player documentation.
- Identifying red flags or suspicious behavior.
- Escalating suspicious cases promptly.
- Ensuring customer information remains accurate and up to date.
- Following all KYC and CDD procedures.

4.3 FRAUD AND RISK TEAMS

The Fraud and Risk Teams are responsible for:

- Monitoring transactional behavior.
- Investigating suspicious activities.
- Applying account restrictions where necessary.
- Collaborating with Compliance on high-risk accounts.

4.4 MANAGEMENT

Management is responsible for:

- Supporting compliance initiatives.
- Ensuring adequate staffing and resources.
- Promoting a culture of compliance and ethical conduct.

5. CUSTOMER IDENTIFICATION REQUIREMENTS

Prior to establishing a customer relationship, the company must obtain sufficient information to verify the player's identity. Only fully registered players may access or use

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

the Company's gaming services. Players who fail to complete the registration process shall not be permitted to play, deposit, wager, or withdraw funds.

The following information must be collected:

- Full legal name
- Date of birth
- Residential address
- Nationality
- Email address
- Phone number
- Government-issued identification number

Acceptable forms of identification may include:

- Passport
- National ID card
- Driver's license
- Residence permit

Players who do not register an account and complete the required registration details will not be permitted to play.

6. IDENTITY VERIFICATION PROCEDURES

The Company shall complete customer identification and verification procedures prior to permitting withdrawals and before allowing account activity that exceeds internal risk thresholds.

Or:

- Before first withdrawal,
- Before cumulative deposits exceed threshold,
- Before triggering risk indicators.

Verification procedures may include:

- Document verification
- Biometric verification
- Liveness detection
- Address verification
- Database screening
- Device and behavioral analysis
- Payment method ownership verification

The company reserves the right to request additional documentation at any time.

Anonymous, fictitious, or numbered accounts are strictly prohibited.

7. RISK-BASED CUSTOMER DUE DILIGENCE

The company applies a risk-based approach to customer due diligence.

Players are categorized into risk levels including:

- Low Risk
- Medium Risk
- High Risk

Risk classification may consider:

- Player location
- Payment methods used
- Transaction patterns
- Occupation or industry
- Source of funds
- Source of wealth
- PEP status
- Sanctions exposure
- Account behavior
- Fraud indicators

KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.

The procedure for Gathering Information can be found in “Procedure for Sanctions and PEP Screening”, which is an integral part of the KYC Policy.

The Company shall gather and assess information regarding the purpose and intended nature of the business relationship in order to develop an appropriate customer risk profile. Information may be obtained through customer declarations, transaction history analysis, bank statements, payment method analysis, open-source intelligence, public registers, adverse media searches, and other reliable independent sources.

The Company shall assess the expected level and nature of customer activity, including anticipated transaction frequency, expected deposit levels, source of funds, source of wealth, gaming behavior, occupation, and geographic exposure.

Medium and High-Risk customers shall be subject to enhanced ongoing monitoring, including periodic reviews conducted on a risk-sensitive basis and event-triggered reviews where unusual activity or material changes are identified.

8. ENHANCED DUE DILIGENCE (EDD)

EDD measures must be applied when higher risks are identified.

8.1 SITUATIONS REQUIRING EDD

EDD may be required for:

- Politically Exposed Persons (PEPs).
- High-risk jurisdictions.
- Unusual transaction patterns.
- Large or inconsistent deposits/withdrawals.
- Adverse media findings.
- Sanctions matches.
- Structuring activity.
- Multiple linked accounts.
- Third-party payment activity.

8.2 ADDITIONAL EDD MEASURES

Additional measures may include:

- Source of funds verification (information on the nature of and details concerning the customer's business, occupation and employment, or any other activity from which the customer derives his/her wealth (e.g., inheritance).
- Source of wealth verification (the expected source and origin of the funds to be used throughout the business relationship and the anticipated level and nature (including expected value and frequency of transactions) that is to be undertaken throughout the relationship).
- Additional identity documentation.
- Video verification interviews.
- Senior management approval.
- Enhanced transaction monitoring.
- Independent database verification.

9. ONGOING MONITORING

Customer relationships must be continuously monitored to identify suspicious or unusual activity.

Monitoring activities include:

- Reviewing transaction activity.
- Monitoring deposits and withdrawals.
- Reviewing changes in customer behavior.
- Identifying linked or duplicate accounts.
- Monitoring sanctions and PEP status updates.
- Conducting periodic account reviews.

The company may request updated documentation periodically or when triggered by risk indicators.

10. SANCTIONS AND PEP SCREENING

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

Sanctions screening is performed prior to onboarding and before establishing the business relationship. We also conduct ongoing sanctions rescreening on a risk-based basis and upon specific events (including changes to customer data, payment method updates, unusual activity, threshold events, or other risk indicators). As a minimum, sanctions rescreening is performed daily for automated list updates and upon each withdrawal request (or other material transaction event), and additionally whenever event-triggered reviews occur.

We screen customers against, at minimum, United Nations (UN) sanctions lists and European Union (EU) sanctions lists, and any other applicable sanctions/watchlists required by Curaçao law and regulatory expectations (including, where applicable, OFAC or other relevant lists).

Potential matches are reviewed promptly by Compliance. Where a match is confirmed, the account will be restricted and/or terminated in accordance with applicable laws and regulations, and the matter will be escalated for compliance determination of any reporting obligations.

The company shall screen players against:

- International sanctions lists.
- Government watchlists.
- Terrorism financing databases.
- Politically Exposed Person databases.
- Adverse media sources.

Potential matches must be reviewed promptly by Compliance.

Accounts associated with confirmed sanctions matches shall be restricted or terminated in accordance with applicable laws and regulations.

The sanctions and PEP screening procedure is established in the document 'Procedure for Sanctions and PEP Screening', which forms an integral part of this KYC and CDD Policy.

11. SOURCE OF FUNDS AND SOURCE OF WEALTH

The company may request documentation demonstrating the legitimacy of a player's source of funds or wealth.

Trigger	Threshold
Basic KYC	Before first withdrawal
SOF Review	EUR 2,000–5,000 cumulative deposits
Enhanced SOF	EUR 5,000+
SOW Review	EUR 10,000+ lifetime deposits
Mandatory EDD	EUR 15,000+ or High Risk
Crypto EDD	EUR 1,000–2,000 equivalent
PEP EDD	Immediately upon identification

Examples may include:

- Bank statements.
- Pay-slips.
- Tax returns.
- Business ownership documents.
- Investment records.
- Crypto wallets
- Property sale agreements.
- Inheritance documentation.

Failure to provide satisfactory documentation may result in account restrictions or closure.

12. SUSPICIOUS ACTIVITY REPORTING AND ESCALATION

Employees must immediately escalate suspicious activity to the Compliance or Fraud Team.

Examples of suspicious activity include:

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

- Structuring transactions to avoid thresholds.
- Use of third-party payment methods.
- Inconsistent player explanations.
- Rapid movement of funds.
- Fraudulent documentation.
- Identity discrepancies.
- Unusual betting or gaming patterns.
- Multiple linked accounts.

Employees must not disclose to player that an investigation or report has been filed.

13. RECORD RETENTION

Records shall be retained for at least five (5) years following the termination of the business relationship and for such longer period as may be required under applicable laws, regulations, regulatory directives, litigation, hold requirements, or instructions from competent authorities.

Records may include:

- Customer identification documents.
- Verification results.
- Transaction histories.
- Communication records.
- Internal investigation notes.
- Compliance approvals.

Records must be stored securely and protected from unauthorized access.

14. DATA PROTECTION AND CONFIDENTIALITY

Player information collected under this policy must be handled in accordance with applicable privacy and data protection laws.

The company shall:

- Protect customer data confidentiality.
- Restrict access to authorized personnel.
- Use secure storage and transmission methods.
- Maintain appropriate cybersecurity safeguards.

Player information shall only be shared where legally permitted or required.

15. TRAINING AND AWARENESS

Employees involved in player onboarding, payments, fraud prevention, or compliance activities must receive periodic KYC/AML training.

Training topics may include:

- AML and KYC regulations.
- Fraud detection.
- Suspicious activity indicators.
- Escalation procedures.
- Sanctions compliance.
- Data privacy obligations.

Training records shall be maintained by the company.

16. NON-COMPLIANCE

16.1 PLAYER NON-COMPLIANCE

Failure to comply with this policy may result in:

Account suspension for KYC refusal, or if not complied with within 30 days of KYC request, until the player complies.

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

Where a player reaches an applicable deposit threshold that triggers additional CDD/KYC (including SOF/SOW and/or EDD requirements), the Company will request the required documentation and may apply interim restrictions while verification is pending. If the required CDD/KYC documentation is not satisfactorily received and verified within thirty (30) days from the date the applicable threshold is reached, the Company may restrict gameplay and transactions, suspend the account and/or terminate the business relationship, and—where required by law or regulatory obligations—freeze or withhold funds pending compliance review. Any such case will be escalated to Compliance for determination of next steps, including whether reporting to competent authorities is required.

Permanent account closure and possible confiscation of funds, for submitting false or digitally altered documents.

The Company reserves the right to suspend, restrict, or terminate accounts where satisfactory KYC documentation is not provided or where fraudulent, false, or manipulated documentation is identified, subject to applicable laws, regulatory obligations, and the Company's Terms and Conditions.

16.2 EMPLOYEE NON-COMPLIANCE

Failure to comply with this policy may result in:

- Disciplinary action.
- Regulatory penalties.
- Legal liability.
- Employment termination.

Intentional violations or attempts to circumvent controls may be escalated for further investigation.

17. POLICY REVIEW AND UPDATES

This policy shall be reviewed periodically and updated as necessary to reflect:

**KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE POLICY
KING ENTERPRISES N.V.**

- Regulatory changes.
- Operational changes.
- Emerging financial crime risks.
- Internal audit findings.
- Industry best practices.

The Compliance Department is responsible for maintaining the current version of this policy.

APPENDIX A – EXAMPLES OF ACCEPTABLE DOCUMENTS

Proof of Identity

- Passport.
- Driver's license.
- National ID card.
- Residence permit.

Proof of Address

- Utility bill.
- Bank statement.
- Government correspondence.
- Tax document.

Source of Funds

- Pay-slips.
- Bank statements.
- Business income documentation.
- Tax returns.

APPENDIX B – EXAMPLES OF RED FLAGS

- Multiple accounts using shared payment methods.
- Frequent changes to account information.
- Transactions inconsistent with player profile.
- Refusal to provide documentation.
- Use of anonymizing tools or VPNs in suspicious contexts.
- Deposits and withdrawals with minimal activity.
- Chargeback abuse.
- Rapid account turnover.
- Suspicious linked accounts.
- Unusual geographic activity.

APPENDIX C – ESCALATION WORKFLOW

1. Employee identifies suspicious activity.
2. Case is documented internally.
3. Case is escalated to Fraud, Compliance, or the AML Compliance Officer.
4. Additional review and investigation are conducted where appropriate.
5. Account restrictions or enhanced monitoring measures may be applied.
6. Where required, unusual or suspicious activity may be reported to the Financial Intelligence Unit of Curaçao (“FIU Curaçao”) through the applicable goAML or FIU reporting system.
7. Final decisions, escalations, and reporting references shall be documented and retained.
8. Employees and authorized personnel are prohibited from disclosing the existence of investigations, suspicious activity reviews, FIU reports, or related reporting obligations to affected customers or unauthorized third parties.