

Know Your Customer Policy

Cura Casino B.V.

Section 1 → Purpose & Scope

I will now draft the **first section** fully professional/legal-grade:

1. Purpose and Scope

1.1 Purpose

This *Know Your Customer (KYC) Policy* establishes the framework of mandatory procedures, processes and controls that Cura Casino B.V. (hereinafter referred to as "the Company") shall implement to ensure that it meets and exceeds all applicable legal and regulatory requirements concerning the identification and verification of its Players, the ongoing monitoring of their activity, and the proper management, suspension, and closure of Player accounts.

This Policy is designed to fully align with:

- The National Ordinance on the Reporting of Unusual Transactions (NORUT)
- The National Ordinance Identification when Rendering Services (NOIS)
- The Sanctions National Ordinance
- The Kingdom Sanctions Act
- The Regulations for Combating Money Laundering, Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction
- Curaçao Gaming Control Board (GCB) Guidelines, Circulars, and Communications
- The Financial Action Task Force (FATF) Recommendations (as applicable)
- The EU 5th AML Directive principles (as benchmark best practices)
- General Data Protection Regulation (GDPR) as applicable to the Company's operations and data processing
- The Company's internal **Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Policy**

The objectives of this Policy are to:

- Establish and verify the identity of all Players prior to providing gaming services.
- Ensure that Players' identities are continuously verified and monitored commensurate with risk.

- Prevent the misuse of the Company's gaming platform for the purposes of money laundering, terrorist financing, and other forms of financial crime.
- Promote transparency and accountability in Player account management.
- Define the process for the lawful suspension and closure of Player accounts.
- Preserve the integrity of the Company's services and reputation.

1.2 Scope

This Policy applies to:

- All **natural persons** or **legal persons** (if legally permitted) registering for a Player account and using the Company's gaming services.
- All Company business units, departments, and employees involved in Player onboarding, account management, transaction monitoring, compliance, legal, and customer support.
- All relevant third-party service providers engaged by the Company for the purpose of KYC, AML screening, or transaction monitoring services.
- All processes, procedures, and internal controls related to Player identification, verification, monitoring, account suspension, and closure.

This Policy is mandatory and binding upon:

- All Company directors and officers.
- The Money Laundering Reporting Officer (MLRO) and Deputy MLRO.
- All employees and staff of the Company.
- Contractors, agents, and affiliates where applicable.

1.3 Relationship with other Policies

This KYC Policy is to be read and applied in conjunction with the following Company policies and procedures:

- **Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy**
- **Data Protection and Privacy Policy**
- **Responsible Gaming Policy**
- **Client Acceptance Policy**

- **Transaction Monitoring Procedures**
- **Sanctions Screening and PEP Screening Procedures**
- **Suspicious Transaction Reporting Procedures**

Where conflicts or inconsistencies arise, the **AML/CFT Policy** shall prevail unless expressly stated otherwise in applicable law or regulation.

2. Definitions

For the purposes of this Policy, the following definitions shall apply:

“Player”

A natural person who registers and maintains an account with the Company for the purpose of participating in remote gaming services offered under license no: OGL/2024/1839/1071 issued by the Curaçao Gaming Control Board.

“Know Your Customer (KYC)”

A set of legally mandated and risk-based processes and procedures implemented by the Company to identify, verify, and monitor the identity and activity of Players, to assess the legitimacy of their source of funds and source of wealth, and to ensure ongoing compliance with applicable AML/CFT laws and regulations.

“Customer Due Diligence (CDD)”

The process of verifying the identity of a Player, including understanding the nature and purpose of the Player’s relationship with the Company and monitoring that relationship on an ongoing basis to ensure it is consistent with the Company’s knowledge of the Player and the Player’s risk profile.

“Enhanced Due Diligence (EDD)”

Additional verification and monitoring measures applied to Players who are assessed to present a higher risk of money laundering or terrorist financing. EDD measures shall include obtaining additional information on the Player’s source of wealth, source of funds, and/or conducting more frequent and detailed ongoing monitoring.

“Politically Exposed Person (PEP)”

A natural person who is or has been entrusted with prominent public functions, including heads of state or government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, and important political party officials, as well as their immediate family members and close associates, whether domestic or foreign.

“Sanctions List”

Any list of designated individuals, entities, groups, or countries subject to financial sanctions imposed under applicable United Nations Security Council Resolutions (UNSCRs), European Union regulations, the Kingdom Sanctions Act, OFAC lists, or other applicable national or supranational sanctions regimes.

“Negative Media”

Publicly available information or intelligence, whether proven factual or alleged, related to financial crime, organized crime, terrorism, trafficking, cybercrime, regulatory misconduct, or any predicate offenses for money laundering or terrorist financing, which would give rise to concerns about a Player’s suitability.

“Suspension of Player Account”

The temporary deactivation of a Player’s account and the restriction of the Player’s access to Company services pending further investigation or the satisfaction of compliance requirements.

“Closure of Player Account”

The permanent termination of the Player’s relationship with the Company, including the closure of the Player’s account, the cessation of all services provided to the Player, and the retention of the Player’s data in accordance with applicable laws.

“Source of Funds (SOF)”

The origin of the particular funds used by a Player to deposit and wager on the Company’s platform.

“Source of Wealth (SOW)”

The origin of the Player’s overall wealth, including the activities or business from which the Player derives their entire net worth.

“Ongoing Monitoring”

The continuous process of reviewing and analyzing Player transactions and behavior to detect and report any unusual or suspicious activity, and to ensure that Player activity remains consistent with the Company’s knowledge of the Player and the Player’s risk profile.

“Company”

Cura Casino B.V., a limited liability company established under the laws of Curaçao and operating remote gaming services under pending License to be issued by the Curaçao Gaming Control Board.

3. Player Identification and Verification

3.1 General Principles

The Company adopts a **risk-based approach** to the identification and verification of Players, fully aligned with applicable AML/CFT laws, the Curaçao Gaming Control Board (GCB) Guidelines, and FATF Recommendations.

The Company shall:

- Prohibit the establishment of anonymous or fictitious Player accounts.
- Identify and verify the identity of every Player prior to allowing any deposit, gameplay, or withdrawal activity.
- Apply **Customer Due Diligence (CDD)** measures commensurate with the assessed risk profile of each Player.
- Apply **Enhanced Due Diligence (EDD)** measures where higher risk is identified.
- Maintain secure records of all identification and verification data.
- Ensure that no account activity occurs until the Player has successfully completed the required KYC procedures.

3.2 Timing of Verification

- Verification of identity and screening procedures must occur **prior to allowing the first deposit**.
- If a Player’s identity cannot be verified within a reasonable period, the Company shall:
 - Immediately suspend the account.
 - Prevent any further deposit or gameplay activity.
 - Initiate the account closure procedure if verification is not completed.
- Ongoing verification and monitoring shall occur throughout the life of the Player relationship.

3.3 Player Identification Data Requirements

Upon registration, the Player must provide, at a minimum:

- Full legal name.
- Date of birth.
- Place of birth.
- Nationality.
- Permanent residential address (including building number, street name, city, country, and postal/ZIP code).
- Email address.
- Mobile phone number.

The Player shall be required to confirm that all information provided is accurate and complete.

3.4 Verification of Identity and Address

The Company shall verify the identity and address of every Player using **reliable and independent source documents**, data, or information.

Acceptable Proof of Identity Documents:

- Valid unexpired **passport**.
- Valid unexpired **national identity card** issued by a government authority.
- Valid unexpired **residence permit** (if applicable).
- Valid unexpired **driving license** (accepted only if permitted under applicable law and only when residential address is included).

Acceptable Proof of Residential Address Documents:

- Utility bill (electricity, gas, water, landline telephone) dated within the last 6 months.
- Bank or financial institution statement dated within the last 6 months.
- Official government correspondence (e.g. tax bill, municipal certificate) dated within the last 6 months.

- Rental or lease agreement (signed and dated) clearly indicating the Player's residential address.

Where a document does not include all required details, supplementary documents may be requested.

3.5 Verification Process

Manual Verification:

- A trained member of the Company's KYC or Compliance team shall manually review and validate all identity and address documents provided by the Player.
- **Liveness verification** shall be conducted through:
 - A **selfie** submitted by the Player holding the identity document.
 - Where required, real-time video verification using third-party tools.
- The reviewer shall ensure that:
 - The document is valid and unaltered.
 - The photograph matches the Player.
 - The address is consistent with the Player's declared country of residence.

Automated Screening:

- All Players shall be automatically screened at onboarding using **ComplyAdvantage** or equivalent service for:
 - Politically Exposed Persons (PEPs).
 - Sanctions List inclusion.
 - Negative Media.
- Crypto wallet screening shall be conducted using **Chainalysis** or equivalent for Players depositing in Virtual Assets.

3.6 Identification of Beneficial Owners

- Where a Player acts on behalf of another person or entity (if permitted under applicable law), the Company shall identify and verify the beneficial owner(s) in accordance with the AML/CFT Policy.

- The same level of identification and verification shall apply to each beneficial owner as to the Player.

3.7 Third-Party Reliance

- The Company may rely on third-party KYC/AML service providers only where:
 - A formal agreement is in place.
 - The third party is regulated under equivalent AML/CFT standards.
 - The Company retains ultimate responsibility and control.
- All third-party providers shall be audited regularly by the MLRO.

3.8 Record Keeping

The Company shall retain complete records of:

- All identification data submitted by Players.
- Verification results and related correspondence.
- Screening results (PEP, Sanctions, Negative Media).
- Beneficial ownership checks (where applicable).
- Ongoing monitoring and review notes.

All records shall be:

- Stored securely in encrypted format.
- Maintained for **at least five (5) years** from the date of account closure or termination of the business relationship.
- Accessible to the MLRO, Deputy MLRO, and relevant authorities upon lawful request.

4. Player Management

4.1 General Principles

The Company is committed to managing Player accounts in accordance with:

- Legal and regulatory requirements under Curaçao AML/CFT laws.
- FATF Recommendations.
- Best practices in responsible gaming and data privacy.
- The Company's **AML/CFT Policy**, **Client Acceptance Policy**, and **Responsible Gaming Policy**.

Player management encompasses the continuous monitoring of Player behavior and transactional activity to:

- Ensure consistency with the Player's risk profile.
- Detect unusual or suspicious patterns.
- Protect the integrity of the Company's operations.
- Uphold Player rights and data privacy.

4.2 Risk-Based Approach to Player Management

The Company employs a **risk-based approach** to Player management, whereby the level and frequency of monitoring and review is determined by:

- The Player's assigned **Customer Risk Assessment (CRA)** level:
 - Low Risk
 - Medium Risk
 - High Risk
- The Player's transactional behavior.
- The products and services utilized.
- The Player's country of residence.
- The Player's Source of Funds (SOF) and Source of Wealth (SOW).
- Any adverse information identified through PEP/Sanctions/Negative Media screening.
- Internal transaction monitoring alerts.

4.3 Ongoing Monitoring

The Company conducts both **automated** and **manual** ongoing monitoring of Player accounts:

Automated Monitoring:

- Continuous review of all Player deposits, withdrawals, and gameplay activity.
- Automated detection of anomalies, including:
 - Sudden changes in transaction volume or frequency.
 - Transactions inconsistent with the Player's profile.
 - Patterns indicative of layering or structuring.
 - Use of high-risk payment methods.
 - Use of known high-risk jurisdictions.

Manual Monitoring:

- Periodic manual review of Player accounts, with increased frequency for Medium and High Risk Players.
- Ad hoc review triggered by:
 - Automated alert thresholds being exceeded.
 - Negative media hits.
 - Sanctions list updates.
 - Changes in Player profile (e.g. relocation to high-risk jurisdiction).

Frequency of Review:

Risk Level	Manual Review Frequency
Low Risk	Annual
Medium Risk	Semi-annual
High Risk	Quarterly or upon any triggering event

4.4 Updating KYC Information

The Company shall require Players to update their KYC information:

- Upon reaching predefined transactional thresholds.

- Upon change of risk level (e.g. from Medium to High).
- Upon detection of discrepancies in existing information.
- Upon significant change in Player behavior.
- In response to regulatory or legal obligations.

Players must provide updated:

- Proof of Identity.
- Proof of Address.
- Proof of Source of Funds (SOF) and/or Source of Wealth (SOW) where required.

Failure to provide required updates may result in account **suspension** or **closure** (refer to Sections 5 and 6).

4.5 Monitoring of PEP, Sanctions, and Negative Media Status

- All Players are automatically screened **daily** against:
 - PEP Lists.
 - Sanctions Lists.
 - Negative Media databases.
- Screening is conducted via **ComplyAdvantage** or an equivalent screening solution.
- Positive or potential matches are escalated to the MLRO for immediate review.

4.6 Transaction Monitoring and Alerts

The Company operates a **Transaction Monitoring System** that applies pre-defined rules and thresholds based on:

- Player risk profile.
- Historical activity.
- Known typologies of financial crime.

Alerts generated by the system are subject to:

- Initial review by Compliance staff.

- Escalation to MLRO where warranted.
- Recording of review outcomes in the Player's account file.

4.7 Data Privacy and GDPR Compliance

In managing Player accounts, the Company adheres strictly to:

- The General Data Protection Regulation (GDPR), where applicable.
- Local data protection laws in the jurisdictions where Players reside.

Key principles:

- Player data is processed solely for lawful purposes.
- Player data is protected against unauthorized access or disclosure.
- Players have the right to access, rectify, or request deletion of their personal data, subject to AML/CFT record-keeping obligations.
- Data retention periods:
 - **5 years** from the closure of the Player's account or termination of the business relationship, unless longer retention is required by law.

A **Data Protection Impact Assessment (DPIA)** has been conducted for the Player Management process, in consultation with the Company's Data Protection Officer (DPO), where applicable.

4.8 Internal Reporting and Oversight

The MLRO shall report on Player Management processes to the:

- **Risk Committee** on a quarterly basis.
- **Board of Directors** on an annual basis or ad hoc if material risks or breaches are identified.

Reports shall include:

- Summary statistics on Player risk profiles.
- Volume and nature of transaction monitoring alerts.
- PEP/Sanctions/Negative Media hits.
- Suspensions and closures related to KYC/AML triggers.

- Emerging typologies and trends.

4.9 Employee Awareness and Training

All employees involved in Player Management must:

- Complete mandatory AML/CFT and KYC training on an annual basis.
- Complete ad hoc training where required due to changes in regulation or internal procedures.
- Confirm their understanding of this Policy in writing.

Training records shall be maintained by the MLRO.

5. Suspension of Player Accounts

5.1 General Principles

The suspension of a Player account is a **preventive measure** that may be applied by the Company where there is:

- A legal or regulatory obligation to suspend activity.
- A compliance risk that requires temporary restriction of services.
- Reasonable suspicion or knowledge of money laundering (ML), terrorist financing (TF), or other financial crime.
- Non-compliance with the Company's KYC or AML/CFT requirements.
- Other breaches of the Company's Terms & Conditions or Responsible Gaming Policy.

The suspension of a Player account does not automatically imply closure, but rather constitutes a **temporary restriction** pending further investigation or rectification of identified issues.

5.2 Legal Grounds for Suspension

A Player account may be suspended on any of the following grounds:

KYC / AML Non-Compliance:

- Failure to provide required identification and verification documents.

- Failure to update KYC information when requested.
- Failure to provide satisfactory evidence of Source of Funds (SOF) or Source of Wealth (SOW).
- Inability to verify the Player's identity, address, or beneficial ownership (if applicable).

Transactional Red Flags:

- Transactions inconsistent with the Player's risk profile.
- Transactions involving high-risk jurisdictions.
- Structuring or smurfing of deposits or withdrawals.
- Use of anonymous or high-risk payment methods.
- Unexplained changes in transactional behavior.

Screening Triggers:

- Positive or unresolvable PEP match.
- Positive or unresolvable Sanctions List match.
- Negative Media hit indicating possible involvement in predicate offenses for ML or TF.

Suspicious Activity Reporting:

- The MLRO has knowledge or reasonable suspicion that the Player's activity may involve ML, TF, or other financial crime, and filing of a Suspicious Transaction Report (STR) with the FIU is required.

Responsible Gaming Concerns:

- Breach of the Company's Responsible Gaming Policy (e.g. evidence of problem gambling behavior, fraud, or bonus abuse linked to addictive behavior).
- Self-exclusion request by the Player.

Regulatory or Law Enforcement Instruction:

- Receipt of an instruction from the FIU, law enforcement agency, or regulatory authority to suspend the Player's account.

5.3 Suspension Process

The suspension process is governed by principles of **proportionality**, **accountability**, and **due process**:

Initial Suspension Action:

- The relevant team (Compliance / Fraud Prevention / AML Unit) identifies a suspension trigger.
- The matter is escalated to the MLRO for review and authorization.
- Upon MLRO approval, the Player account is immediately suspended in the system.
- All gameplay, deposit, and withdrawal activity is blocked.
- Pending withdrawals may be placed on hold pending investigation.

Internal Record-Keeping:

- The reason for suspension must be clearly documented in the Player account file.
- All supporting evidence (alerts, screening results, correspondence, transaction data) must be retained.

Player Communication:

- The Player shall be notified of the suspension unless doing so would constitute **tipping off** under applicable AML/CFT laws.
- Where notification is provided, it shall state:
 - That the account is suspended.
 - Whether the suspension is temporary pending receipt of required information, or linked to other risk factors.
 - The actions the Player must take to resolve the suspension (if applicable).
- If notification would constitute tipping off, no communication shall be sent; this decision is to be documented and approved by the MLRO.

Timeframe:

- The Company shall aim to resolve suspensions in a timely manner.
- If the Player does not cooperate or the risk remains unresolved, the case shall be escalated to potential **account closure** (Section 6).

5.4 Oversight and Escalation

MLRO Responsibility:

- The MLRO is responsible for oversight of all account suspensions triggered by compliance concerns.
- The MLRO shall:
 - Review all supporting documentation.
 - Ensure that suspension actions are lawful, proportionate, and documented.
 - Escalate matters to the Risk Committee where high reputational or legal risk is involved.

Board Reporting:

- A summary of suspensions linked to AML/CFT concerns shall be reported to the Board of Directors on a quarterly basis.
- High-profile cases may be reported on an ad hoc basis.

5.5 Duration of Suspension

Suspensions shall remain in place until:

- The Player satisfactorily resolves the KYC/AML issue.
- The MLRO determines that the risk is mitigated to an acceptable level.
- Regulatory or law enforcement clearance is obtained.
- The Company determines that closure of the Player account is appropriate (Section 6).

5.6 Player Funds During Suspension

- Player funds shall be safeguarded during the period of suspension.
- No withdrawal shall be permitted where doing so would risk facilitating ML/TF or where an STR has been filed.
- Where legally permissible, and where no STR is involved, withdrawals may be processed subject to enhanced scrutiny and MLRO approval.

5.7 Record Keeping

- Full records of all suspensions, including rationale, documentation, communications, and outcomes, shall be retained for a minimum of five (5) years following resolution.

6. Closure of Player Accounts

6.1 General Principles

The permanent **closure of a Player account** is an action that may be taken by the Company where:

- The Player relationship is deemed unsustainable from a compliance or legal standpoint.
- The Player voluntarily requests closure.
- Regulatory or legal obligations necessitate closure.

Closure actions shall be **proportionate, documented, and legally defensible**, and shall be conducted in accordance with:

- The Company's **AML/CFT Policy**.
- The **Client Acceptance Policy**.
- Relevant Curaçao AML/CFT legislation.
- The National Ordinance on the Reporting of Unusual Transactions (NORUT).
- GCB Guidelines.
- The General Data Protection Regulation (GDPR), where applicable.

Closure of an account **terminates the Player's relationship** with the Company and permanently disables the Player's access to all gaming services.

6.2 Legal Grounds for Closure

Voluntary Closure:

- The Player submits a formal request to close their account.
- The Player initiates permanent self-exclusion under the Company's Responsible Gaming Policy.

KYC / AML / CFT Compliance:

- The Player fails to provide satisfactory KYC/EDD information after repeated requests.
- The Player provides false, forged, or misleading documentation or information.
- The Player is unable to demonstrate a legitimate Source of Funds (SOF) or Source of Wealth (SOW).
- The Player is conclusively identified as a Sanctions List subject.
- The Player is conclusively identified as a PEP whose risk cannot be mitigated to an acceptable level.
- The Player is the subject of Negative Media involving predicate offenses to ML/TF.
- The MLRO files an STR and determines that continued engagement with the Player is untenable.

Transactional Activity:

- Persistent transactional patterns indicative of ML/TF.
- Activity involving prohibited third-party accounts or payment methods.
- Transactions inconsistent with the Player's declared profile and activity.

Regulatory or Law Enforcement Instruction:

- Receipt of an instruction or order from:
 - The FIU.
 - A law enforcement agency.
 - The GCB.
 - A competent court.

Breach of Terms & Conditions:

- Breach of the Company's Responsible Gaming Policy.
- Fraudulent activity, including bonus abuse, collusion, or chargeback fraud.
- Attempted circumvention of KYC/AML controls.

6.3 Closure Process

Initiation:

- The closure process may be initiated by:
 - The MLRO.
 - Compliance / AML Unit.
 - Responsible Gaming Unit (for voluntary closure/self-exclusion).
 - Legal Department (for regulatory orders).
 - Player request.

Review and Approval:

- All forced closures linked to AML/CFT concerns must be approved by the MLRO.
- High-risk closures must be escalated to the Risk Committee if:
 - Reputational risk is involved.
 - Potential legal action is foreseeable.

Execution:

- The Player account is permanently disabled in the Company's systems.
- All gameplay, deposit, and withdrawal functionality is terminated.
- The Player is notified of closure, subject to **tipping off** restrictions under AML/CFT laws.
- If tipping off applies, no communication is sent; this must be documented and MLRO-approved.

Notification to Player:

Where notification is legally permissible, the Player shall be informed:

- That their account is closed.
- That they may not re-register under a different identity.
- That their data will be retained as required by law.
- Where relevant, of the right to appeal the closure (except where prohibited by law or where closure is linked to a regulatory/legal instruction).

6.4 Handling of Player Funds upon Closure

- The Company has a duty to act lawfully and with due care in the handling of Player funds.
- Where no STR has been filed and no regulatory freeze applies:
 - Remaining Player funds may be returned to the originating payment method, subject to enhanced review and MLRO approval.
 - Returns of funds must not be made to third-party accounts or unverified payment channels.
- Where an STR has been filed or where legal/regulatory freeze applies:
 - Funds may be frozen and held pending further instruction from the FIU or competent authority.
 - No communication regarding the freeze shall be made to the Player if this would constitute tipping off.

6.5 Record-Keeping Requirements

The Company shall retain comprehensive records of all account closures, including:

- Reason for closure.
- Supporting documentation and analysis.
- MLRO and/or Risk Committee approvals.
- Communications with the Player (if applicable).
- Regulatory filings (if applicable).
- Handling of Player funds.

Retention period: **Minimum five (5) years** from the date of closure.

6.6 Reporting Obligations

- Where closure is linked to suspicion or knowledge of ML/TF:
 - An STR shall be filed with the FIU in accordance with the Company's STR procedure.
- Where closure follows a regulatory or law enforcement instruction:
 - Confirmation of compliance shall be provided to the requesting authority as required.

6.7 Prohibition on Re-Registration

- A Player whose account has been closed for AML/CFT, sanctions, or legal risk reasons shall be **prohibited from re-registering** with the Company.
- The Player's identity shall be retained on the Company's internal exclusion and monitoring lists.
- Any attempted re-registration shall trigger an automatic block and escalation to Compliance and the MLRO.

6.8 Oversight and Reporting

- The MLRO shall maintain oversight of all closure actions linked to compliance risk.
- Summary statistics and trends shall be reported to:
 - The **Risk Committee** quarterly.
 - The **Board of Directors** annually.
- Patterns indicative of emerging risks shall be documented and used to update risk assessment processes.

7. Governance, Oversight & Review

7.1 General Principles

The effective implementation of this **Know Your Customer (KYC) Policy** requires strong internal governance, clear assignment of responsibilities, robust oversight mechanisms, and a documented process for regular review and continuous improvement.

The Company recognizes that KYC is not a static process but a dynamic function that must adapt to:

- Changes in Player behavior and typologies.
- Changes in applicable legal and regulatory requirements.
- Developments in technology and payment methods.
- Evolving best practices in AML/CFT risk management.

7.2 Roles and Responsibilities

Board of Directors

The Board of Directors of the Company retains **ultimate responsibility** for ensuring that:

- The Company's KYC framework is fit for purpose.
- Sufficient resources are allocated to the KYC and AML/CFT functions.
- The Company operates in full compliance with applicable AML/CFT laws and regulations.

The Board shall:

- Approve this Policy and any subsequent updates.
- Review quarterly and annual reports on KYC performance and risk.
- Provide strategic direction regarding KYC and AML/CFT risk appetite.

Money Laundering Reporting Officer (MLRO)

The MLRO is responsible for:

- The day-to-day implementation of this Policy.
- Oversight of all KYC processes, including identification, verification, monitoring, suspension, and closure of Player accounts.
- Approving risk-based decisions on Player acceptance, enhanced due diligence, and account closure.
- Acting as the primary liaison with the FIU, GCB, and law enforcement regarding KYC/AML/CFT matters.
- Ensuring that KYC-related Suspicious Transaction Reports (STRs) are timely and properly filed.
- Keeping abreast of changes in applicable AML/CFT laws and emerging typologies.

Deputy MLRO

The Deputy MLRO shall:

- Support the MLRO in all aspects of their role.
- Act in the capacity of MLRO during any period of absence.

Compliance / AML Unit

The Compliance / AML Unit shall:

- Conduct manual reviews of KYC files and transactions.
- Perform ongoing monitoring of Player activity.
- Handle alerts generated by the Transaction Monitoring System.
- Manage the screening of Players against PEP, Sanctions, and Negative Media lists.
- Provide reports to the MLRO for escalation and action.

Risk Committee

The Risk Committee shall:

- Receive and review quarterly reports on KYC performance, emerging risks, and trends.
- Provide guidance on risk appetite and high-risk cases.
- Approve material changes to the KYC framework.

Legal Department

The Legal Department shall:

- Advise on legal aspects of KYC implementation.
- Assist in interpreting regulatory requirements.
- Support the Company's response to legal challenges related to Player suspensions or closures.

IT / Security Department

The IT / Security Department shall:

- Ensure the integrity, security, and availability of KYC data.
- Implement access controls to prevent unauthorized access to Player identification data.
- Support automated screening and monitoring solutions.
- Conduct periodic system audits.

7.3 Policy Review Cycle

This Policy shall be subject to:

- **Annual Review** by the MLRO and Risk Committee.
- Ad hoc review where:
 - Material changes in legal or regulatory requirements occur.
 - Emerging risks or typologies are identified.
 - Changes in the Company's business model, products, or markets occur.

Following each review:

- Updates shall be presented to the Board of Directors for approval.
- Revised versions of the Policy shall be communicated to all relevant staff.

7.4 Internal Audits

- The Company shall conduct **internal audits** of its KYC processes on at least an annual basis.
- Audits shall assess:
 - Adherence to this Policy.
 - Effectiveness of controls.
 - Accuracy of record-keeping.
 - Staff training and awareness.
 - Compliance with applicable AML/CFT laws.
- The MLRO shall document all audit findings and monitor the implementation of corrective actions.

7.5 Training and Awareness

All employees involved in KYC processes shall:

- Complete mandatory AML/CFT and KYC training **at least annually**.
- Undergo additional training where material changes in the Policy occur.
- Confirm in writing their understanding of this Policy and their personal responsibilities.

Training shall cover:

- KYC and CDD procedures.
- Transaction monitoring.
- Emerging ML/TF typologies.
- Tipping off risks.
- Data protection obligations.

Training records shall be maintained by the MLRO.

7.6 Record-Keeping Principles

The Company shall maintain comprehensive records of:

- Player identification and verification data.
- Ongoing monitoring records.
- Risk assessments and screening results.
- Records of suspensions and closures.
- STR filings and related correspondence.
- Internal audit reports and corrective actions.
- Training records.

Retention period: **Minimum five (5) years** from the date of account closure or termination of the business relationship, or longer where required by applicable law.

Records shall be:

- Securely stored in encrypted format.
- Accessible only to authorized personnel.
- Available for inspection by competent authorities upon lawful request.

7.7 Continuous Improvement

The Company is committed to:

- Regularly assessing the effectiveness of its KYC controls.
- Benchmarking against industry best practices.

- Leveraging new technologies to enhance KYC effectiveness.
- Proactively identifying and mitigating new and emerging risks.