Anti-Money Laundering and Countering the Financing of Terrorism

VERSION CONTROL AND POLICY REVIEW HISTORY

Date of Adoption	Version and Description	Approved/Reviewed by
February 20, 2026	Version 1 – Adoption of the Policy	Board

This Anti-Money Laundering and Counter-Terrorist Financing ("AML/CTF") Policy sets out the standards, controls, and procedures adopted by the Company in its capacity as a **B2C gaming operator**, providing betting services to Players either directly or through an approved network of Agents. The Policy serves as the governing framework for all staff, employees, Agents, and Senior Management, supporting the effective identification, prevention, and management of money laundering and terrorist financing risks. It is aligned with international best practices, including FATF recommendations and applicable igaming regulatory expectations.

1. INTRODUCTION

The rise of online gaming has created both new opportunities and heightened financial crime risks. As a licensed **B2C gaming operator,** Precise Interactive Inc. (the "**Company**") is committed to protecting its platform from being misused for money laundering (ML), terrorist financing (TF), or any other form of criminal activity. The Company's AML/CFT controls apply to both fiat and virtual asset / crypto-denominated transactions, wallets, payment channels, and settlement mechanisms supported by the Platform.

This Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy establishes the Company's framework for identifying, preventing, and reporting ML/TF risks in accordance with applicable laws, licensing conditions, and regulatory expectations under the applicable laws. The Policy is aligned with international best practices, including the standards set by the Financial Action Task Force (FATF). Specific misuse typologies addressed by this Policy include, without limitation, chip dumping, collusion, multi-account fund passing, wallet pass-through activity, coordinated table behaviour, bonus abuse, rapid deposit-withdraw cycles, and tournament manipulation patterns. This Policy also covers risks relating to sanctions breaches, proliferation financing, and restricted-jurisdiction access, including cross-border payment flows and wallet activity.

This Policy is a living document and will be reviewed at least annually, or more frequently when required due to changes in regulation, operational processes, or emerging risks. All employees, senior management, **Agents**, and other relevant third parties are expected to understand and comply with the obligations set out in this Policy.

Failure to comply may expose the Company and its employees to regulatory, criminal, financial, and reputational consequences. Any suspected breaches or concerns must be reported immediately to the Company's appointed Money Laundering Reporting Officer (MLRO).

This Policy applies across the Company's operational lifecycle, including **Agent onboarding, Player onboarding, screening, transaction monitoring, payouts, and ongoing oversight of the Agent network**, ensuring that robust AML/CFT safeguards are embedded at every stage.

2. Objectives of the AML/CFT Policy

The objective of this AML/CFT Policy is to establish clear internal standards and procedures to prevent, detect, and respond to money laundering, terrorist financing, and other forms of financial crime. This Policy demonstrates the Company's commitment as a B2C gaming operator to maintaining the integrity of its platform, complying with applicable regulatory requirements, and safeguarding its services from misuse by Players or Agents.

The specific objectives of this Policy are to:

1. Ensure compliance with all applicable AML and CFT laws, as well as international best practices including the FATF Recommendations.

2. Ensure compliance with applicable international sanctions, trade restriction, and counter-proliferation financing regimes, including UN, EU, UK, and US sanctions frameworks, and to prevent Platform misuse by sanctioned persons or entities.
3. Define the roles and responsibilities of personnel involved in AML/CFT compliance, including the MLRO, senior management, employees, and Agents.
4. Establish risk-based procedures for onboarding, verifying, and monitoring Players, including Customer Due Diligence (CDD) requirements.
5. Set thresholds and requirements for Enhanced Due Diligence (EDD), Source of Funds (SoF), and Source of Wealth (SoW) verification.
6. Provide clear guidance for identifying, escalating, and reporting suspicious activity, including internal reporting protocols and the submission of Suspicious Activity Reports (SARs).
7. Promote a culture of compliance and ethical behavior among employees, senior management, and approved Agents operating under the Company's framework.
8. Implement ongoing monitoring measures, including automated and manual reviews, to detect suspicious or unusual transactions and behaviors.
9. Support transaction chain tracing and fund-flow analysis across wallets, accounts, poker tables, and related gaming activity to detect fund passing, chip dumping, layering, and coordinated abuse patterns.
10. Outline the documentation, record-keeping, and audit trail requirements necessary to support regulatory oversight and law enforcement cooperation.
11. Maintain structured cooperation with regulators, Financial Intelligence Units (FIUs), supervisory authorities, and law enforcement bodies.
12. Require regular training for employees and Agents to ensure awareness of ML/TF risks, red flags, and internal reporting responsibilities. Provide for periodic independent audit and external or internal compliance review of AML/CFT controls, systems, and procedures to validate effectiveness and identify control gaps.
13. Establish enforcement measures for non-compliance with this Policy, including disciplinary actions or termination of relationships with individuals or Agents. Ensure continuous improvement of AML/CFT controls through ongoing risk assessment updates, control testing, model tuning, and policy refinement based on audit findings, regulatory developments, and emerging typologies.

This Policy forms a key component of the Company's broader compliance framework and will be reviewed periodically to ensure it remains effective and proportionate to emerging risks.

3. Definition of Money Laundering and Terrorist Financing

Money laundering refers to the process by which individuals or entities conceal the origins of illicitly obtained funds in order to make them appear legitimate. Terrorist financing involves the provision or collection of funds intended to be used to carry out terrorist acts, regardless of whether the funds are of lawful or unlawful origin. In the context of online gambling, poker, and casino platforms, money laundering and terrorist financing risks may also arise through virtual asset transactions, and cross-platform value transfers, where blockchain-based assets, tokens, or digital currencies are used to obscure fund origin or movement.

The stages of money laundering typically include:

- **Placement:** Introducing illicit funds into the financial system, such as through deposits, gambling activity, or currency exchanges.
- **Layering:** Conducting a series of financial transactions to obscure the origin of the funds, such as converting them into different instruments or transferring them between multiple accounts.
- **Integration:** Reintroducing the laundered funds into the legitimate economy through investments, purchases, or other seemingly lawful means.

Terrorist financing often mimics the structure of money laundering but may involve funds derived from legal sources. It consists of:

- **Collection:** Gathering funds through donations, legitimate earnings, or criminal activity.
- **Transmission:** Moving funds across accounts, borders, or platforms.
- **Utilization:** Spending the funds to support terrorist acts, recruit members, purchase materials, or propagate ideologies.

Online gambling and gaming typologies may include bonus abuse, coordinated low-risk wagering, deposit–withdrawal cycling, minimal-risk betting strategies designed to legitimize funds, and promotional fund recycling without genuine gameplay intent. Poker-specific laundering typologies may include chip dumping, soft play between colluding accounts, intentional loss transfers, table manipulation, coordinated tournament play, and peer-to-peer value transfer disguised as gameplay outcomes. “Mule accounts” or “account passing” refers to the use of third-party or nominee accounts to deposit, wager, transfer, or withdraw funds on behalf of another person in order to conceal true ownership or control of funds. The use of mixers, tumblers, privacy tools, or obfuscation services refers to techniques or services designed to hide blockchain transaction trails will be treated as a heightened AML risk indicator.

Both activities pose significant threats to the financial system and the integrity of the gaming industry. The Company recognizes its duty to identify and report any suspected ML or TF activity through proper internal controls, staff training, and reporting mechanisms in accordance with applicable laws and regulations.

4. Regulatory Framework and Applicable Laws

This Policy has been prepared in accordance with the applicable AML and CFT laws and regulations guided by international best practices and standards, including those established by the Financial Action Task Force (FATF). The Company also considers relevant guidance issued by regional and global regulatory bodies to ensure its controls are robust, responsive, and proportionate. The Company operates under a recognized gaming license framework and is subject to AML/CFT supervision and compliance expectations applicable to licensed gaming operators. The Company acknowledges its obligation to cooperate with the relevant Financial Intelligence Unit (FIU) and other designated reporting authorities in relation to suspicious transaction reporting and AML/CFT information requests.

The Company acknowledges that as a licensed B2C gaming operator, it may be exposed to customers, transactions, and risks originating from different jurisdictions. Therefore, it adopts a unified compliance framework that draws from the following sources:

1. Recommendations and standards issued by the Financial Action Task Force (FATF).
2. Applicable AML/CFT legislation and regulatory guidance.
3. Guidance published by Tier 1 jurisdictions, such as the UK Gambling Commission (UKGC), Malta Gaming Authority (MGA), and EU directives, where relevant.
4. Global sanctions regimes and asset freezing obligations, including those issued by:
    - The United Nations Security Council (UNSC)
    - The United Kingdom's Office of Financial Sanctions Implementation (OFSI)
    - The European Union (EU)
    - The United States Department of the Treasury (OFAC)

The Company maintains a sanctions compliance framework designed to prevent dealings with sanctioned persons, entities, wallets, and jurisdictions, including asset freeze and no-benefit requirements where applicable under sanctions laws and regulatory expectations.

5. Internal risk assessments and enterprise-wide AML/CFT risk management practices.

Where the Company supports crypto-assets, virtual assets, or blockchain-based payment rails, the Company recognizes evolving global standards applicable to virtual asset service providers (VASPs), including Travel Rule–related data expectations and transaction traceability principles, and will implement proportionate controls consistent with regulatory and industry best practice. The Company undertakes to continuously monitor changes in applicable laws, regulations, and FATF guidance, and to update its AML/CFT procedures accordingly. All AML-related systems and controls shall reflect the prevailing regulatory expectations, even where such expectations are higher than the local legal minimums.

5. Roles and Responsibilities

Effective implementation of this AML/CFT Policy requires clearly defined roles and responsibilities across all levels of the Company. This includes the appointment of a designated Money Laundering Reporting Officer (MLRO), oversight by Senior Management, and ongoing AML/CFT awareness among employees, Agents, and relevant third parties. AML/CFT governance includes defined escalation chains, documented decision authorities, and segregation between operational, commercial, and compliance decision-making roles.

5.1 Money Laundering Reporting Officer (MLRO)

The MLRO is the designated individual responsible for overseeing the Company's AML/CFT compliance framework as a B2C gaming operator. The MLRO shall have the independence, resources, and authority necessary to perform their duties, including direct access to senior management. The MLRO shall operate with functional independence and shall not be subordinated to revenue-generating or customer acquisition functions in the performance of AML/CFT duties. The MLRO shall have a direct reporting line to the Board of Directors or

equivalent governing body and shall have unrestricted access to senior decision-makers for AML/CFT matters.

The MLRO's responsibilities include:

- Ensuring the Company complies with applicable AML/CFT laws and regulatory requirements.
- Receiving, investigating, and assessing internal Suspicious Activity Reports (SARs) and submitting external reports to the Financial Intelligence Unit (FIU), where required.
- Acting as the primary point of contact for regulators, auditors, and law enforcement regarding AML/CFT matters.
- Conducting ongoing reviews of AML/CTF systems, controls, and monitoring procedures.
- Overseeing internal AML/CFT training programs for employees and Agents.
- Ensuring timely updates to this AML/CFT Policy and associated risk assessment methodologies.
- The MLRO is authorised to directly contact regulators, supervisory authorities, and Financial Intelligence Units on behalf of the Company in relation to AML/CFT reporting, enquiries, and cooperation matters.
- The MLRO shall maintain documented escalation and decision logs for suspicious activity cases, regulatory reports, and high-risk account determinations.
    - Deputy MLRO
    - The Company shall designate a Deputy MLRO or alternate compliance officer to act in the MLRO's absence, with delegated authority to receive internal reports, apply urgent controls, and submit regulatory reports where timelines require.
    - Delegation arrangements and authority limits for the Deputy MLRO shall be documented and approved by Senior Management or the Board.

5.2 Senior Management

Senior Management has overall responsibility for establishing and promoting a strong culture of AML/CFT compliance within the Company.

Their responsibilities include:

- Providing oversight and strategic direction for the Company's AML/CFT program.
- Appointing a qualified MLRO and supporting them in fulfilling their duties.
- Reviewing and approving AML/CFT policies, procedures, and risk assessments.
- Ensuring adequate staffing, resources, and tools are allocated to AML/CFT functions.
- Ensuring that operational practices such as onboarding, transaction monitoring, and payout controls follow a risk-based approach.
- Senior Management shall receive periodic AML/CFT compliance reports from the MLRO, including risk metrics, suspicious activity statistics, control deficiencies, and remediation status. Where applicable, Senior Management may constitute or appoint a Compliance or Risk Committee to oversee AML/CFT effectiveness and control performance.

5.3 Employees and Customer-Facing Personnel

All employees involved in customer onboarding, Player verification, transaction monitoring, payments, or support activities must:

- Understand and follow the Company's AML/CFT obligations and procedures.
- Complete mandatory AML/CFT training and periodic refreshers.
- Identify unusual or suspicious Player behavior and escalate such activity to the MLRO immediately.
- Cooperate with internal reviews, audits, or regulatory inquiries when required.
- Employees must follow documented AML/CFT escalation chains and shall not suppress, delay, or override compliance escalations for commercial or customer experience reasons.

5.4 Agents, Affiliates and Third-Party Providers

Agents, marketing affiliates, and other third-party partners who introduce Players or interact with the Company's platform must adhere to this AML/CFT Policy and any additional requirements communicated by the Company.
The Company reserves the right to:

- Conduct due diligence on such parties;
- Request information or documentation to assess AML/CFT risk;
- Suspend or terminate partnerships where AML/CFT concerns or non-compliance are identified.

AML/CFT responsibility cannot be outsourced, and while operational tasks may be delegated to Agents or third parties, ultimate AML/CFT accountability remains with the Company. Third parties performing AML-relevant functions must be subject to defined escalation, reporting, and cooperation obligations toward the MLRO and compliance function.

6. Customer Due Diligence (CDD) and Know Your Customer (KYC)

Customer Due Diligence (CDD) is a core component of the Company's AML/CFT framework and involves collecting, verifying, and maintaining accurate information about **Players** to assess potential ML/TF risks.

The Company applies a **risk-based CDD process** upon: (a) the Players meeting the thresholds as determined by the Company from time to time in line with the periodic business risk assessment carried out by the Company ("**CDD Threshold**"); and (b) any suspicious activity being identified or if the Company has a reasonable apprehension of any suspicious activity. CDD applies **only to Players**, while Agents undergo a separate due diligence process appropriate for business partners

6.1 Timing and Triggers for CDD

CDD must be conducted on a Player when:

- The Player reaches the applicable CDD Threshold.
- There is suspicion of ML/TF, fraud, or identity misuse.
- There is doubt about the accuracy, legitimacy, or completeness of previously collected KYC data.

Additional CDD triggers apply where blockchain analytics, device intelligence, or fraud monitoring tools assign elevated risk scores to a Player or funding instrument.

6.2 Information to be Collected

The following information must be collected at the onboarding stage:

- Full legal name
- Date of birth
- Nationality
- Residential address (supported by proof of address)
- Email address and mobile number
- Occupation and, where relevant, employer
- Source of Funds (SoF) when threshold or risk triggers apply
- Valid government-issued photo ID (passport, national ID, driver's license

6.3 Document Verification Requirements

- Identification documents must be valid, legible, and issued by a recognized authority.
- Proof of address must be recent (issued within the last six (6) months).
- Verification may be completed manually or through approved electronic verification systems.
- Any mismatches or inconsistencies must be escalated and resolved before enabling withdrawals.
- The Company may, in its sole discretion, apply payment method ownership checks, to ensure that deposit and withdrawal methods are held or controlled by the same Player identified through KYC.

6.4 Ongoing CDD and Refresh Cycles

CDD must be refreshed when:

- There is a material change in the Player's behavior, deposit pattern, betting pattern, or risk profile.
- The Player changes their country of residence or primary payment method.
- Identification documents on file expire.
- A Player is flagged for suspicious activity or requires Enhanced Due Diligence (EDD).

The Company performs periodic reviews based on Player risk level (e.g., annual for low-risk, more frequent for higher-risk Players).

6.5 CDD Failures and Account Restrictions

When a Player fails to provide complete or verifiable CDD information:

- Withdrawal privileges shall be suspended.
- The account may be restricted or frozen where legally permitted.
- The MLRO must be informed of repeated failures or suspicious circumstances.
- The Company may offboard the Player or file an external Suspicious Activity Report (SAR), if appropriate.
- Accounts may also be restricted where wallet ownership cannot be verified, payment instruments fail ownership matching checks, or blockchain risk scores exceed internal acceptance thresholds.

6.6 Prohibited and Restricted Players

The Company shall not onboard or continue to service any Player who:

- Is under the age of 18 (or the jurisdiction's minimum legal age).
- Fails identity verification after reasonable attempts.
- Appears on relevant sanctions or PEP lists, unless permitted under strict controls.
- Resides in jurisdictions prohibited by the Company's policy or licensing conditions.

All CDD and KYC documentation, verification logs, and review notes shall be retained securely for a minimum of **five (5) years** after the end of the Player relationship or longer if required by regulation. Sanctions screening, PEP screening, and adverse media screening are conducted upon players triggering the CDD Threshold and periodically thereafter upon the Player being classified as a high-risk Player, using approved screening databases and tools. Players connecting from prohibited or high-risk jurisdictions based on IP, device, network, or geo-location intelligence may be blocked, restricted, or subject to enhanced verification. Multi-account detection controls, including device linkage and behavioral correlation tools, may be used to prevent duplicate, mule, or pass-through accounts.

7. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is required when a **Player** presents a heightened risk of money laundering or terrorist financing. EDD provides additional assurance regarding the Player's identity, financial background, and legitimacy of funds used for gambling.

7.1 EDD Triggers

EDD must be conducted when any of the following apply:

- The Player reaches the **EDD Threshold** (e.g., cumulative deposits or net settlements of GBP 100,000 within a rolling 365-day period).
- The Player is identified as **high-risk** based on onboarding information, Player behavior, transaction patterns, or monitoring alerts, including rapid stake escalation, abnormal tournament buy-in frequency, or disproportionate chip movement between related poker accounts.
- The Player is identified as a **Politically Exposed Person (PEP)** or has links to high-risk jurisdictions.
- There is concern regarding the legitimacy or sufficiency of the Player's Source of Funds (SoF) or Source of Wealth (SoW).
- EDD is triggered where high-value or high-frequency crypto asset flows are observed into or out of a Player account (based on data provided by licensed third party crypto service providers) , including clustered or structured blockchain deposits.
- EDD is mandatory where blockchain analytics tools indicate exposure to mixers, tumblers, privacy-enhancing services, or obfuscation protocols.
- EDD is required where blockchain or transaction monitoring systems assign elevated chain risk scores to wallet addresses or funding sources.

7.2 EDD Measures

The Company shall apply one or more of the following EDD measures, depending on risk:

- Obtaining enhanced or certified identity documentation.
- Collecting additional documentation to verify Source of Funds (e.g., bank statements, payslips, contracts, tax documents).
- Assessing the Player's Source of Wealth (e.g., business income, inheritance, assets, investments).
- Conducting enhanced screening, including open-source intelligence (OSINT) and adverse media reviews.
- Validating that the Player's occupation, income, and financial profile align with observed gambling behavior.
- Requiring real-time video verification or equivalent high-assurance identity verification methods.

EDD measures may include blockchain transaction tracing, wallet clustering analysis, and chain-of-funds review using approved blockchain analytics providers. Enhanced poker integrity review measures may be applied, including collusion analysis, chip-dumping detection, and cross-account behavioral linkage checks. EDD measures must be proportionate to the Player's risk level and sufficient to form a reasonable understanding of the Player's financial legitimacy.

7.3 Source of Funds (SoF) and Source of Wealth (SoW)

- **Source of Funds (SoF)** refers to the immediate financial origin of the money used for gaming activity (e.g., salary, savings, bank account transfers).

- **Source of Wealth (SoW)** refers to the overall origin of the Player's accumulated wealth and financial standing (e.g., business ownership, investments, inheritance).

The Company must be satisfied that documentation is adequate, reliable, and consistent with the Player's activity and risk profile.

7.4 Escalation and Approval

- All EDD reviews and documentation must be assessed and approved by the **MLRO** or a designated senior compliance officer.
- Player accounts subject to EDD may remain restricted such as **restricted withdrawals or limited activity** until the review is completed.
- Cases where information is incomplete, inconsistent, or raises concern must be escalated to the MLRO for further review, possible account suspension, or external reporting.
- Final approval for continuation of any high-risk relationship subject to EDD must be documented and expressly approved by the MLRO or a senior compliance authority designated by the MLRO. Where risk remains elevated after EDD, senior management approval may additionally be required before account restrictions are lifted.

7.5 Recordkeeping

All EDD records including risk assessments, supporting documentation, internal notes, and rationale for decisions must be securely retained for at least **five (5) years**, or longer where required by law or regulation. EDD-reviewed accounts shall be subject to mandatory periodic re-review at defined intervals based on risk rating. Enhanced monitoring flags and EDD status markers must remain active in monitoring systems until formally cleared by Compliance.

8. Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function, as well as their immediate family members and known close associates. Due to their heightened exposure to corruption, public funds, and influence, PEPs present an inherently elevated risk of money laundering. For risk-classification purposes, PEPs are further categorized as foreign PEPs, domestic PEPs, and international organization PEPs, with foreign PEPs generally treated as presenting higher inherent risk. The Company applies a risk-based distinction between domestic and foreign PEP exposure when determining onboarding outcomes and control intensity, subject to MLRO override.

8.1 Identification of PEPs

The Company must screen all **Players and Agents** during onboarding and on a periodic basis using reliable screening tools to determine whether they are PEPs or related to PEPs.

Categories of PEPs include:

- Heads of state or government, senior politicians, senior government, judicial, or military officials.
- Senior executives of state-owned enterprises.
- Key political party officials.
- Immediate family members (e.g., spouse, parents, siblings, children).
- Close associates known to have joint beneficial ownership or close business relationships.
- The definition of close associates includes beneficial co-owners, known business partners, trustees, nominee shareholders, and persons exercising joint control over financial or business arrangements with the PEP. PEP screening shall include sanctions lists, regulatory watchlists, adverse media databases, and specialized PEP intelligence databases provided by approved vendors.

8.2 Prohibition on Onboarding PEPs

- If a Player or Agent is identified as a PEP or associated with a PEP during onboarding, they shall not be onboarded.
- The MLRO must document the decision and ensure the account is rejected prior to any transactional activity.
- Where applicable law or license conditions permit exceptions, onboarding of a PEP may only occur under documented MLRO approval, mandatory Enhanced Due Diligence, verified Source of Wealth, and senior management sign-off.

8.3 Handling Existing Accounts Identified as PEPs

If an individual is identified as a PEP after onboarding:

- The account must be immediately restricted and escalated to the MLRO.
- A risk assessment must be conducted to determine the nature of the exposure.
- Unless there is a compelling and well-documented justification approved by the MLRO, the relationship must be terminated.
- Any suspicious indicators must be reviewed for potential SAR filing.
- Verified PEP accounts that are exceptionally permitted to continue must be subject to mandatory Enhanced Due Diligence, verified Source of Wealth and Source of Funds, and enhanced ongoing transaction monitoring. Enhanced monitoring controls for PEP accounts shall include lower alert thresholds, increased transaction review frequency, and mandatory compliance review of significant deposits and withdrawals. Continued relationships with PEPs must be re-approved periodically by the MLRO and documented with updated risk rationale.

8.4 Ongoing Screening and Controls

- PEP screening tools must be kept updated to ensure accurate detection.
- Employees and Agents must be trained to recognize PEP red flags.
- Any potential PEP matches must be escalated and reviewed before action is taken.

- PEP status must be re-screened upon material account changes or major transaction events.

9. Risk-Based Approach

The Company adopts a **Risk-Based Approach (RBA)** consistent with international AML/CFT standards, including FATF Recommendations. This approach ensures that resources, controls, and monitoring efforts are applied proportionately to the money laundering or terrorist financing risks posed by different **Players, transaction types, products, and jurisdictions**. The Company maintains and documents an enterprise-wide AML/CFT risk assessment covering Players, products, poker and casino game formats, payment channels, delivery channels, agents, affiliates, and jurisdictions. This assessment is approved by Senior Management and reviewed at least annually. The enterprise-wide risk assessment incorporates both fiat and crypto transaction exposure, cross-border platform access risk, and poker-specific integrity risks such as chip-dumping, collusion, and peer-to-peer value transfer patterns.

9.1 Risk Categories

The Company classifies risks across the following key categories:

- **Player Risk -** Based on identity information, behavioral patterns, funding methods, Source of Funds, PEP/sanctions exposure, and any adverse indicators.
- **Geographic Risk** - Based on the Player's country of residence, IP location, payment origin, and exposure to sanctioned, high-risk, or FATF-listed jurisdictions.
- **Transaction Risk** - Based on deposit behavior, frequency, betting activity, withdrawal patterns, use of multiple payment instruments, and deviations from the Player's expected profile.
- **Product / Channel Risk** - Based on features of remote gaming, reliance on Agents, online account creation, and payment methods offered by the Company. Channels with reduced face-to-face interaction may present elevated risks.
- Product Risk scoring is applied across poker-first and secondary casino products, including cash tables, tournaments, peer-to-peer formats, jackpot features, and bonus-driven products, with higher risk scores assigned to features that enable rapid value transfer or low-friction fund cycling . Payment Channel Risk scoring is applied across all supported deposit and withdrawal methods, including cards, bank rails, e-wallets, prepaid instruments, and crypto assets, with differentiated controls applied based on reversibility, traceability, and third-party funding exposure.
- Crypto Asset Risk scoring is applied to blockchain-based deposits and withdrawals, taking into account asset type, wallet behaviour, chain analytics risk indicators, mixer exposure, and exchange-of-origin signals based on data provided by licensed third party crypto service providers.
- Agent and Affiliate Channel Risk scoring is applied where Player acquisition or transaction activity is linked to agents or marketing partners, including concentration risk, abnormal player clustering, and abnormal gameplay fund flows.

9.2 Risk Assessment Process

Each Player is assigned a risk rating at the point when CDD is triggered and reassessed periodically thereafter. Risk ratings are based on Player information, behavior, monitoring alerts, and internal or external data sources. The Company classifies Players into:

- **Low Risk**: Standard CDD requirements apply; monitoring follows normal thresholds.
- **Medium Risk**: Increased monitoring frequency and earlier refresh triggers may apply.
- **High Risk**: Subject to mandatory EDD, additional documentary requirements, and closer ongoing monitoring by Compliance and the MLRO.

Risk ratings are dynamic and may change as new information becomes available.

9.3 Risk Scoring and Profiling

The Company uses a combination of **automated tools** and **manual compliance reviews** to assess Player risk. Scoring models and behavioral analytics may flag accounts or transactions for further review based on indicators such as:

- Unusually high deposit or wagering activity.
- Discrepancies between reported occupation/income and gambling behavior.
- Matches against sanctions, PEP, or adverse media lists.
- Use of higher-risk payment channels or third-party accounts.
- Rapid movement of funds or patterns suggestive of layering or fund passing.
- Blockchain analytics risk scores (Third-Party tools and data consolidation), wallet exposure ratings, device intelligence risk indicators, and behavioural poker gameplay anomaly signals
- Poker-specific behavioural risk indicators may include abnormal chip transfer patterns, repeated soft-play indicators, coordinated table behaviour, and rapid balance equalisation patterns across linked accounts.

Flagged accounts are reviewed by the Compliance Team and escalated where necessary.

9.4 Mitigating Measures

To manage and mitigate identified risks, the Company implements:

- **Identity verification controls**, including document and biometric authentication tools.
- **Ongoing transaction monitoring**, powered by risk-based thresholds and alerts.
- **Enhanced Due Diligence (EDD)** for high-risk Players or unusual activity.
- **Escalation and SAR protocols** for cases with ML/TF suspicions.
- **Account restrictions**, such as deposit limits, withdrawal holds, or full suspension pending review.
- **Agent oversight measures**, including periodic reporting and review of Player activity in their downlines.

These measures ensure that higher-risk scenarios receive proportionate scrutiny.

Mitigating controls are calibrated according to composite risk scores combining Player, product, payment channel, agent, and jurisdiction risk ratings rather than single-factor triggers.

9.5 Periodic Review and Updates

The Company's **Risk Assessment Matrix**, tools, and methodologies are reviewed at least annually by the MLRO and Senior Management, or earlier if:

- new regulatory requirements arise;
- emerging risks are identified;
- internal audits or monitoring reveal control gaps;
- product or operational changes occur.

Updates are implemented promptly to ensure continued effectiveness and proportionality.

10. Ongoing Monitoring and Reporting of Suspicious Activity

The Company maintains robust monitoring procedures to ensure that **Player activity** is continuously reviewed for indicators of money laundering, terrorist financing, fraud, or other financial crime. Ongoing monitoring enables the Company to detect unusual or suspicious behavior and take timely action. Monitoring controls include both fiat and blockchain-based transaction monitoring.

10.1 Ongoing Monitoring

All Player activity is monitored to ensure it is consistent with the Player's known risk profile, expected behavior, and declared source of funds. Monitoring applies to transactional activity, login behavior, betting patterns, and any changes in Player circumstances.

Key triggers for review include:

- Unusually large or frequent deposits/withdrawals
- Early, repeated, or rapid withdrawals without proportional gameplay
- Use of third-party or unrelated payment methods
- Geographic anomalies, such as logins or deposits from high-risk or sanctioned jurisdictions
- Rapid turnover of funds, including deposit–withdraw cycles suggestive of layering or fund passing
- Behavioral inconsistencies (e.g., sudden increases in stake size or activity)

Additional monitoring triggers include rapid in/out funding patterns, structured deposit patterns designed to avoid CDD/EDD thresholds, repeated near-threshold transactions, and circular value movement across linked accounts. Poker-specific laundering indicators are monitored, including chip-dumping patterns, soft-play coordination, repeated heads-up transfer behaviour, coordinated tournament value transfer, and abnormal chip flow

between related accounts. Bonus abuse and promotion laundering indicators are monitored, including multi-account bonus capture, low-risk wagering purely to clear bonus balances, and coordinated bonus extraction behaviour. Activity originating from or linked to **Agents** may also be reviewed where Player patterns raise concerns.

10.2 Transaction Monitoring Tools

The Company uses automated monitoring tools designed to:

- Detect predefined red-flag scenarios
- Generate alerts for unusual transactions or behavior
- Identify patterns inconsistent with the Player's profile

Alerts are reviewed by trained AML/Compliance personnel, who determine whether escalation or further investigation is necessary.

Automated monitoring using third party service providers is supplemented by manual checks where risk or anomalies warrant closer scrutiny. Automated monitoring scenarios include mixer and tumbler detection controls, high-risk wallet clustering alerts, exchange-of-origin flags, and abnormal chain-hop patterns.

10.3 Internal Reporting Procedures

Employees and Agents must immediately escalate any suspicion or reasonable grounds to suspect ML/TF activity through an internal **Suspicious Activity Report (SAR)** submitted to the MLRO.

An internal SAR should include:

- Player details and account history
- Description of the suspicious activity and observed red flags
- Supporting documentation or screenshots
- Date, time, and context of how the suspicion arose

The MLRO maintains a secure SAR register and assesses each report to determine appropriate actions. Internal SAR submissions must be assigned a unique case reference number for tracking, review, and audit trail purposes. Employees and Agents must not conduct independent investigations beyond preliminary fact capture and must escalate to the MLRO promptly without alerting the Player.

10.4 External Reporting to Authorities

If the MLRO determines that external reporting obligations are met, a formal SAR must be filed with the **Financial Intelligence Unit (FIU)** or relevant authority in.

All filings must:

- Follow legally required timelines

- Use the prescribed reporting format
- Be submitted through the designated channel or system

The MLRO is responsible for all statutory reporting decisions. Where crypto or cross-border transaction indicators are involved, SAR narratives should include wallet addresses, transaction hashes, chain analytics risk indicators, and linked account references where available.

10.5 Recordkeeping and Confidentiality

- All SARs, internal investigation notes, and supporting documents must be securely retained for at least **five (5) years** or longer where required by law.
- Employees and Agents are strictly prohibited from informing any Player or third party that a SAR has been filed or investigated (tipping off).
- Breaches of confidentiality or failure to escalate suspicious activity may result in disciplinary action and potential legal consequences.
- Alert reviews, investigation steps, decision rationale, and SAR filing determinations must be fully documented to an alert disposition standard sufficient for regulatory and audit reconstruction. Alert disposition records must include reviewer identity, review date, evidence considered, decision outcome, and escalation path taken.

10.6 Manual Review and Escalation

In addition to automated monitoring, the Company performs manual reviews for:

- High-risk Players
- EDD cases or SoW/SoF documentation gaps
- Discrepancies or inconsistencies in identity documents
- Adverse media findings
- Suspicious activity linked to specific Agent networks

The MLRO has final authority regarding the classification, escalation, or external reporting of any suspicious activity.

The Company operates a documented AML case management workflow covering alert intake, triage, investigation, MLRO escalation, SAR decisioning, regulator reporting, and post-case monitoring flags. Case workflow stages, status changes, and approval checkpoints are logged to maintain a complete supervisory audit trail.

11. Affiliates and Third-Party Arrangements

The Company may engage external parties such as affiliates, marketing partners, payment processors, and technology vendors to support its B2C gaming operations. While these partnerships contribute to commercial growth and customer acquisition, they also create potential AML/CFT exposure if not appropriately managed. All third-party arrangements must align with the Company's internal controls and legal obligations. All affiliates, payment

processors, and third-party service providers must comply with AML/CFT, sanctions, and financial crime prevention obligations equivalent to those applied by the Company, proportionate to their role and risk exposure. Third-party risk assessments must consider jurisdiction, service type, transaction exposure, data access level, crypto handling capability, and prior regulatory or enforcement history.

11.1 Affiliate Oversight

Affiliates play a role in introducing Players to the platform and must operate in a manner fully consistent with the Company's AML/CFT standards. The Company requires all affiliates to:

- Adhere to the Company's guidelines on responsible marketing and customer targeting.
- Refrain from promoting in **prohibited or high-risk jurisdictions**.
- Avoid misleading, aggressive, or inappropriate advertising practices.
- Promptly report unusual Player sign-up patterns, suspicious behavior, or fraud indicators to the Company.

Affiliates must provide AML and sanctions compliance representations and warranties confirming that their marketing practices, traffic sources, and player acquisition methods do not involve prohibited jurisdictions, sanctioned persons, or deceptive identity practices. Affiliate agreements must include jurisdictional marketing restrictions, including express prohibition on targeting or onboarding players from restricted or sanctioned territories. Affiliates must agree to provide cooperation, data access, and supporting records where required for AML, fraud, collusion, or bonus abuse investigations. The Company may conduct **periodic reviews or audits** of affiliate activity to ensure compliance with contractual and regulatory obligations.

Any affiliate found to present unacceptable AML/CFT or reputational risk may have its agreement suspended or terminated, and may be reported to relevant authorities where required.

11.2 Due Diligence on Third Parties

Before onboarding a third-party provider with access to Player data, financial flows, or compliance-critical functions, the Company conducts appropriate due diligence, including:

- Identification of the provider's ownership and controlling persons.
- Assessment of the provider's AML/CFT controls, security frameworks, and regulatory status.
- Screening of the entity and its key individuals against sanctions, PEP, and adverse media databases.

Contracts with third-party providers must include provisions requiring:

- Compliance with applicable AML/CFT laws and Company standards.
- Cooperation with investigations, reviews, or audits initiated by the Company.
- Prompt reporting of any incidents that may affect Player safety, data integrity, or AML compliance.
- Payment processors and wallet infrastructure providers must demonstrate active AML programs and, where applicable, provide AML certification, regulatory licensing evidence, or equivalent compliance attestations. Third-party providers must be contractually required to perform sanctions and watchlist screening on relevant counterparties where they handle identity, payments, or wallet infrastructure

11.3 Outsourcing and Delegation

Where the Company outsources operational tasks with AML relevance such as identity verification, sanctions screening, or transaction monitoring it retains **ultimate responsibility** for compliance. Outsourcing contracts must include regulator access clauses, cooperation duties, and immediate incident notification obligations for AML, sanctions, fraud, or data integrity events.

Outsourced partners must:

- Demonstrate adequate systems, controls, and regulatory compliance.
- Undergo periodic performance reviews and updated risk assessments.
- Cooperate fully with internal audits, external audits, and regulator inquiries.

Outsourcing must never result in weakened oversight, reduced control, or gaps in AML/CFT compliance.

11.4 Recordkeeping and Termination

The Company maintains complete documentation of all due diligence conducted on affiliates and third-party service providers.

Partnerships may be suspended or terminated immediately if they:

- Present an unacceptable AML/CFT or fraud risk
- Fail to meet contractual or regulatory obligations
- Refuse to cooperate with compliance reviews or audits

The Company affirms that no third-party arrangement may be used to bypass, weaken, or outsource statutory AML/CFT responsibilities. Oversight, accountability, and traceability must be preserved across all external relationships. Third-party and affiliate contracts must include express AML audit rights allowing the Company or its appointed auditors to review compliance controls, records, and relevant procedures on reasonable notice. Failure by an affiliate or vendor to meet AML, sanctions, or fraud control obligations constitutes grounds for immediate suspension or termination without notice.

12 Employee Training and Awareness

The Company recognizes that effective training and awareness are essential to the success of its AML/CFT program. Employees must understand how to identify, respond to, and escalate potential money laundering, terrorist financing, and financial crime risks within a B2C gaming environment.

12.1 Mandatory Training

All employees involved in compliance, finance, operations, customer support, or who have access to Player information or financial transactions must complete AML/CFT training upon joining the Company and at least annually thereafter, with additional training provided for high-risk roles or in response to regulatory changes.

Additional training may be required for high-risk roles or when regulatory changes occur.

12.2 Training Objectives

The AML/CFT training program shall ensure that employees are able to:

- Understand the Company's AML/CFT obligations and the purpose of this Policy.
- Identify red flags associated with **Player behavior**, Agent linked activity, or potential fund passing.
- Understand Player risk profiles, CDD and EDD triggers, and escalation channels.
- Properly submit internal Suspicious Activity Reports (SARs) to the MLRO.
- Recognize the disciplinary, civil, and criminal consequences of non-compliance.

12.3 Training Methods

Training may be delivered through virtual or in-person workshops, policy briefings supported by case studies and scenario-based exercises, as well as compliance circulars, newsletters, and regulatory updates.

12.4 Documentation and Monitoring

The MLRO shall maintain detailed records of:

- Training materials and content used.
- Completion logs for each employee.

Completion of AML/CFT training is a **condition of employment**. Repeated failure to complete training or comply with requirements may result in disciplinary action.

12.5 Training for Third Parties

Where applicable, the Company may extend AML/CFT awareness programs or minimum standards to **Agents and Affiliates** who perform functions with AML relevance.

This may include:

- Onboarding briefings for Agents and Affiliates.
- Training on red flags, reporting obligations, and prohibited activities.
- Refreshers aligned with regulatory expectations.

Training effectiveness shall be periodically reviewed and updated based on emerging risks, regulatory changes, and internal audit findings.

13 Record Keeping

Proper record keeping is essential for demonstrating compliance with AML/CFT requirements, supporting investigations, and responding to regulatory audits or law enforcement inquiries. The Company must maintain complete, accurate, and accessible records relating to **Players, Agents**, and AML-relevant activities.

13.1 Retention Period

The Company shall retain the following records for a minimum period of **5 years** from the end of the **Player relationship** or the date of the last transaction, whichever is later:

- Player identification and verification documents (KYC).
- Agent onboarding and due diligence documentation.
- Source of Funds (SoF) and Source of Wealth (SoW) documentation.
- Transaction records, including deposits, withdrawals, betting activity, and gameplay logs sufficient to reconstruct Player behavior.
- Internal and external Suspicious Activity Reports (SARs) and related correspondence.
- AML training logs, audit reports, compliance reviews, and risk assessments.

Records must be maintained in a manner that enables the Company to demonstrate adherence to regulatory requirements at any time.

13.2 Format and Accessibility

Records may be stored electronically or physically but must:

- Be readily retrievable without undue delay.
- Be protected from unauthorized access, loss, or alteration.
- Be indexed and organized to allow efficient retrieval during internal reviews, audits, or regulatory inspections.

13.3 Confidentiality and Data Protection

All AML/CFT-related records are confidential and may only be accessed by authorized personnel. The Company ensures compliance with applicable data protection laws through controlled access, secure retention and storage practices, and the proper deletion of records once legally permitted at the end of the retention period. Any unauthorized disclosure or misuse of AML-related records is strictly prohibited and may result in disciplinary or legal consequences.

13.4 Third-Party Records

Where third-party service providers perform Player onboarding, identity verification, payment processing, or other AML-relevant functions, the Company shall ensure that they maintain equivalent record-keeping and retention standards, provide full and timely access to records upon request, and implement adequate security and confidentiality safeguards. All third-party agreements must expressly grant the Company the right to obtain such records and require the provider to support investigations or audits as needed.

14 Sanctions Screening

The Company is committed to complying with all applicable financial and economic sanctions laws issued by international, regional, and national authorities. Sanctions screening applies to all Players, Agents, and relevant third parties.

14.1 Sanctions Regimes

The Company screens individuals and entities against consolidated sanctions lists issued by authorities such as the United Nations Security Council (UNSC), the European Union (EU), the United Kingdom's Office of Financial Sanctions Implementation (OFSI), the United States Office of Foreign Assets Control (OFAC), and any additional sanctions lists under applicable laws. These sources collectively ensure comprehensive coverage of global restrictions.

14.2 Screening Scope and Frequency

Sanctions screening shall be conducted for Players, Agents, and applicable third parties:

- Once they hit the CDD threshold.
- Upon material changes to a Player or Agent profile (e.g., name, address, payment method, nationality)
- Periodically, in line with ongoing monitoring requirements
- Immediately following updates to sanctions lists or when high-risk alerts are issued

- At any sign of geographic anomalies, such as logins or transactions originating from sanctioned or embargoed jurisdictions

Screening applies to identity information, device/IP data where relevant, and payment instruments.

14.3 Response to Positive or Unresolved Matches

If a sanctions match is identified:

- The account shall be immediately **restricted or frozen** pending verification.
- The case must be escalated to the **MLRO** for assessment.
- If the match is confirmed, the Company shall file a report with the appropriate authority (FIU/sanctions office) and the account shall be permanently blocked.
- No funds shall be released without MLRO approval and regulatory clearance.

If a match cannot be conclusively resolved (an "**unresolved match**"):

- **Enhanced review** must be conducted and documented before allowing any further account activity.
- The MLRO must determine whether to maintain restrictions or proceed with reporting.

The Company shall not onboard or maintain relationships with individuals who appear on sanctions lists.

14.4 Tools and Vendors

The Company uses industry-standard sanctions screening tools capable of automated matching, fuzzy-logic comparisons, and maintaining audit trails. All system-generated alerts undergo manual verification to ensure accuracy and avoid false positives.

14.5 Responsibilities and Oversight

The MLRO ensures that sanctions lists are kept current within the Company's systems, that all alerts and decisions are logged and retained, and that relevant staff receive training on identifying and escalating sanctions-related risks. Failure to comply with sanctions obligations may expose the Company and its personnel to significant legal, regulatory, and reputational consequences.

15 Internal Audit and Compliance Monitoring

To ensure the continued effectiveness of its AML/CFT framework, the Company maintains an internal audit and compliance monitoring program. These mechanisms assess adherence to this Policy, evaluate the effectiveness of controls, and identify areas requiring enhancement.

15.1 Internal Audit Function

The internal audit team, or an appointed third-party auditor, periodically reviews the effectiveness of the Company's AML/CFT controls. The audit process includes evaluating compliance with CDD, EDD, SAR procedures, and record-keeping standards, as well as assessing whether monitoring systems, alert handling, and escalation processes operate effectively. Auditors also review employee training participation, identify weaknesses or gaps in processes, and verify that recommendations from previous audits have been properly implemented. All findings and recommendations are reported to Senior Management and the MLRO with documented follow-up actions and timelines.

15.2 Compliance Monitoring

The AML Compliance Officer (MLRO) is responsible for continuous monitoring of the day-to-day application of AML/CFT controls. This includes:

- Reviewing alerts and escalated cases.
- Verifying timely submission and documentation of SARs.
- Ensuring that updates to laws and regulations are reflected in procedures.
- Coordinating regulatory inspections and requests for information.

15.3 Frequency and Scope

Audit and compliance reviews are conducted at least annually, and ad-hoc reviews may be triggered in response to:

- Material compliance incidents.
- Regulatory changes.
- Business model changes (e.g., new jurisdictions, payment channels).

15.4 Reporting and Action Plans

All audit and compliance findings shall be documented, and corrective action plans shall be prepared in coordination with the relevant departments. Implementation progress must be tracked and verified.

The Company recognizes that effective audit and compliance functions are a regulatory expectation and an integral part of its AML/CFT governance model.