

KYC and AML Code of Conduct

For Anjouan Internet Gaming Operators

Informed by FATF Standards

Final edition | 13 October 2026 | Implementation date specified by AOFA notice

This Code sets operational standards for customer identification, anti-money laundering, counter-terrorist financing and controls against proliferation financing. It provides separate procedures for suspicious activity reports and threshold-based transaction reports.

This edition takes effect only on the date specified in an AOFA adoption notice and applies prospectively. The notice must identify the reporting recipients, secure channels, operational filing format and transitional arrangements before the new reporting procedures commence.

1 Purpose and authority

On adoption, compliance with this Code is a condition of the licences to which AOFA makes it applicable. AOFA means the Anjouan Offshore Financial Authority. Anjouan Gaming means the administrative service designated by AOFA to administer this Code; it is not, by that designation alone, a financial intelligence unit or law-enforcement body.

Operators must comply with applicable law, their licence conditions and binding AOFA directions. This Code supplements those obligations and does not confer authority to disregard another law, licensing restriction, asset-freezing requirement or reporting obligation. Any inconsistency must be escalated promptly to AOFA and resolved without breaching applicable law.

2 Scope and accountability

This Code applies to licensed B2C internet gaming operators, their brands, websites and player accounts. Operators must ensure that their directors, officers, employees, agents and relevant contractors comply with the provisions applicable to their functions. B2B suppliers must provide the records and controls necessary for licensed operators to meet these requirements, within their own applicable licence obligations.

The operator remains accountable when onboarding, payments, monitoring or other compliance functions are outsourced. Contracts must provide timely data access, confidentiality, regulatory access and continuity. Outsourcing must not prevent reporting or inspection.

3 Legal framework and interpretation

This Code is informed by FATF Standards, including the Recommendations and relevant interpretive notes. Those standards inform its design; they are not treated as automatically incorporated domestic law. References to FATF standards and overseas supervisory guidance do not imply FATF endorsement or confer an overseas authorisation.

“Must” creates an obligation under this Code once adopted. “Should” expresses guidance requiring documented consideration. EUR means euros and USD means United States dollars. Unless stated otherwise, deadlines are calendar hours or days and timestamps are recorded in UTC. A reporting threshold is not a safe harbour from due diligence, monitoring or SAR obligations.

4 Governance and core controls

The board or equivalent governing body must approve the AML/CFT programme, risk appetite, resources and material changes. A designated senior manager must oversee implementation. Sales, VIP status and commercial targets must not override compliance decisions.

The operator must appoint a suitably qualified MLRO and deputy with direct access to senior management, necessary records and independent authority to escalate and report concerns. The MLRO may also be the Compliance Officer where resources and independence remain adequate. Report filing must not require commercial approval.

Operators must screen relevant personnel, protect staff who report concerns in good faith and maintain segregation of duties over payments, account adjustments, risk decisions and report approval. The board must receive compliance management information at least quarterly, including overdue reviews, monitoring failures, reporting performance and remediation.

5 Business and player risk assessments

Before commencing operations, and before launching a materially different product, payment channel or technology, the operator must assess the risk of misuse. Review the business assessment at least annually and following material changes or significant incidents. Record methodology, evidence, controls, residual risks and board approval.

- Assess player geography, ownership or control, funding sources, payment channels, agents and intermediaries, product features, speed of funds movement and remote onboarding risks.
- Consider virtual assets, anonymity-enhancing services, cross-border flows, high-value players, third-party funding, account networks and collusive or economically unexplained play.
- Use current AOFA notices and credible jurisdictional risk information. Distinguish sanctions, prohibited markets, FATF high-risk jurisdictions and increased-monitoring jurisdictions; they are not interchangeable categories.

Give each player a documented risk rating at onboarding and update it when activity, identity, geography or risk information changes. Assess combined activity across accounts and brands operated by the same licensee. Controls must reflect the assessed risk and cannot be reduced solely because a player stays below a reporting threshold.

5.1 Screening and targeted financial sanctions

Screen players and relevant counterparties against sanctions applicable under law and AOFA directions before enabling financial activity, when lists change and before payout. Screening may initially use registration information; obtain further identifiers or verification where needed to resolve a match. Resolve potential matches promptly using reliable identifiers. Preserve match evidence and decisions. Apply legally required freezing and reporting without delay; do not release or return blocked funds without lawful authority. A potential name match requires investigation, not automatic permanent confiscation.

5.2 Politically exposed persons

Identify foreign and domestic politically exposed persons, persons entrusted with prominent functions by international organisations, their family members and known close associates. Apply enhanced measures to foreign PEP relationships and to other PEP relationships assessed as higher risk. Obtain senior-management approval, establish source of wealth and funds, and conduct enhanced monitoring. Former officeholders

remain subject to measures while their residual risk warrants them. PEP status alone is not evidence of wrongdoing.

6 Player due diligence standards

6.1 Registration information and threshold based verification

Obtain the player's full legal name, date of birth, residential address and country, nationality, contact details and unique player identifier. No account may be activated until this registration information is supplied.

Documentary identity verification is not routinely required before the first deposit or real-money play under this Code; it becomes mandatory at the triggers in Article 6.2. Apply proportionate age, sanctions and fraud controls at registration. Any earlier verification required by applicable law or a binding licence condition remains mandatory.

Use reliable independent evidence, including valid government photo identification and a recent utility bill or equivalent address evidence, supplemented by appropriate electronic checks. Alternative evidence must be permitted by applicable licence conditions or an AOFA direction; this Code alone does not waive a stricter documentary condition. Where used, electronic identification must be assessed for reliability, independence, fraud resistance and coverage.

At registration, confirm the player acts for their own account. At verification, check document authenticity, consistency and impersonation risk and use additional checks where needed. Do not knowingly permit anonymous accounts, fictitious identities or undisclosed nominee arrangements. Record exceptions and their lawful basis.

6.2 Mandatory identity verification triggers

Complete customer identity, age and residence verification at the earliest of: aggregate lifetime deposits reaching EUR 3,000 or equivalent; the first withdrawal request, regardless of amount; or suspicious activity, regardless of amount. Also verify where a single qualifying financial transaction or an identifiable linked series reaches EUR 3,000 or equivalent, or where previously supplied identity information is doubtful. A cancelled withdrawal request does not remove a trigger.

Complete verification before accepting a deposit that would bring cumulative deposits to or above EUR 3,000, or before executing any other qualifying financial transaction that would reach the EUR 3,000 threshold, either individually or as part of an identifiable linked series. Assess the proposed transaction together with preceding linked operations before execution. Do not wait for a threshold-crossing transaction to be completed before applying the verification requirement. A payment received before verification must be held in a restricted suspense balance, not credited for play or otherwise made available to the player. Permit no further deposits, real-money wagers or payouts until required checks are completed or a lawful resolution is approved. Continue to monitor and report funds actually received, including restricted funds. For unsolicited receipts, apply the same restrictions immediately.

Lifetime deposits are cumulative gross accepted deposits across accounts and brands under the same licensee, without deduction for withdrawals, wagers, losses or refunds. Correct genuine duplicate records through an audit trail. Qualifying financial transactions include funds received or paid, external refunds, exchanges or transfers of withdrawable value and other external financial movements; ordinary internal wagers and recycling of the same gaming balance do not by themselves create additional funds movements. Evaluate linked operations by common player, control or purpose, without an automatic daily reset.

Value each deposit and other qualifying transaction in EUR using the Article 9.3.3 market-rate methodology at the relevant transaction time. Preserve its historical EUR value for cumulative calculations. For a proposed transaction, assess its expected value before acceptance and recheck at execution if exchange-rate movement could affect the trigger. Previously completed reliable verification may be used while it remains current; thresholds do not require repetitive re-verification without a reason.

6.3 Enhanced due diligence and source of funds

Apply EDD where elevated risk is identified, including foreign PEP relationships, other higher-risk PEP relationships, significant adverse information, unusual third-party involvement, high-risk funding channels, suspected structuring, suspicious activity or funding inconsistent with known circumstances. A routine EUR 3,000 threshold or a low-risk first withdrawal triggers CDD verification, not automatic EDD. Record the risk decision and obtain senior-management approval where required.

Review identity and address evidence, obtain an explanation of the activity, and establish the source of funds through evidence proportionate to risk. Assess source of wealth where relevant, particularly for higher-risk PEPs and unexplained substantial funding. Evidence must explain the origin of money used, rather than merely show that money exists in an account. Investigate inconsistencies and document conclusions and approvals.

6.4 Restrictions and ongoing reviews

Once a mandatory Article 6.2 trigger occurs, block further deposits and real-money wagers and do not process withdrawals until required CDD and, where applicable, EDD are completed or a lawful resolution is approved. Where required CDD or EDD cannot be completed, maintain these restrictions. The MLRO must consider whether a SAR is required and whether the relationship should end. Funds must not be confiscated solely because checks are incomplete or a report is filed.

Where the MLRO reasonably believes that seeking further CDD would tip off a person, the MLRO may defer the customer-facing request to the extent permitted by applicable law, record the reason and file the SAR promptly. This does not permit play, deposits, payouts or other activity otherwise restricted by this Code or law, waive verification for future activity, or extend a reporting deadline. Seek lawful direction where necessary.

Review higher-risk relationships at least annually; set documented review cycles for other players according to risk. Refresh information on expiry, material change, doubts about accuracy or an alert. Requests must be proportionate and pursued promptly. Record the reasons for any continued restriction and review them regularly.

7 Payments and player protection

Maintain traceable payment records identifying the payer, payee, account or wallet, instrument, amount, currency, time and status. Before an Article 6.2 verification trigger, check payment ownership against player registration information and available payment-provider information. After verification, check it against verified identity. Escalate discrepancies promptly; complete earlier verification where the discrepancy creates suspicion, identity doubt or elevated risk. This provision does not require routine documentary verification before a below-threshold deposit where no other trigger applies. Prohibit undisclosed third-party funding. Any exceptional payment arrangement requires documented MLRO approval and evidence of lawful ownership, purpose and authority.

Pay withdrawals to a verified account or wallet controlled by the player, ordinarily through the original funding route where lawful and practicable. Alternative routes require verification and a recorded reason. Do not use gaming accounts as general money-transfer or exchange facilities.

7.1 Virtual assets

Assess each supported asset, blockchain, wallet service and payment provider before use. Identify relevant service providers, assess their authorisation where required and apply proportionate blockchain tracing and sanctions controls. For self-hosted wallets, assess control and funding provenance through appropriate evidence; do not assume a wallet is illicit solely because it is self-hosted.

Escalate exposure to illicit services, mixers, theft, fraud, sanctions evasion or unexplained chain-hopping. Apply proportionate limits or refuse activity where risk cannot be mitigated. Retain transaction hashes, network, wallet addresses and valuation records. Comply with travel-rule or transfer-information obligations where legally applicable to the operator or its providers; accepting crypto does not automatically make an operator a licensed virtual-asset service provider.

7.2 Complaints and withdrawal restrictions

Acknowledge player complaints within 72 hours and attempt internal resolution within 30 calendar days. Unresolved eligible disputes must be referred to an AOFA-approved ADR provider at the operator's expense. State the provider and contact details in player-facing terms.

An AML review does not remove ADR obligations, but reporting confidentiality and lawful restrictions must be respected. Explain delays to players to the extent legally permitted without revealing a SAR or prejudicing an investigation. Preserve the complaint and decision record. Filing a CTR alone is not a reason to block a withdrawal.

8 Record keeping

Keep CDD, EDD, screening and relationship records for at least five years after the relationship ends; keep transaction records for at least five years after the transaction. Retain SARs, CTRs, analysis, approvals and filing acknowledgements for at least five years after the relevant report or decision. Apply a longer period where law or a lawful preservation notice requires it.

Records must allow reconstruction of deposits, wagers, withdrawals, transfers, adjustments and refunds, with original currency, EUR and USD valuations where required, timestamps and unique identifiers. Preserve risk decisions, alerts, linkage evidence, training, audits and regulatory correspondence. Use secure, searchable records with access controls, backups and audit trails. Supply records promptly on lawful request, through secure channels.

9 Monitoring and reporting

9.1 Transaction monitoring

Monitor all financial and gaming activity, including attempted, rejected and reversed transactions. Controls must detect split payments, activity just below thresholds, rapid deposits and withdrawals with little play, collusion, unusual betting, multiple accounts, inconsistent geography, third-party funding and unexplained changes in behaviour.

Use real-time controls where needed to prevent or stop high-risk activity and conduct ongoing retrospective analysis. Review relevant activity across rolling 24-hour, 7-day and 30-day periods and longer periods where warranted. Validate data completeness, alert logic and thresholds; document investigations and resolution. A fixed CTR window must never limit broader suspicious-activity monitoring.

9.2 Suspicious activity reports

Report known or suspected money laundering, terrorist financing or related criminal activity promptly and no later than 24 hours after detection of suspicious activity. The deadline runs from when available facts establish suspicion or reasonable grounds for suspicion, not from the later completion of an internal investigation. Routine unexplained alerts require prompt assessment; confirmed suspicion must not wait for commercial or board approval.

Report completed and attempted activity regardless of value and whether an account is closed or a payment refused. Submit to the AOFA-designated secure SAR channel and separately to the competent FIU or other body where applicable law requires. An administrative report does not replace a statutory report. AOFA's adoption notice must identify recipients and channels without describing Anjouan Gaming as an FIU unless legally designated as such.

Include known identities, transaction details, chronology, grounds for suspicion, relevant documents, controls taken and references to related reports. Submit available supporting evidence within the deadline; identify material still being obtained and supplement promptly. Do not delay an initial report to obtain a complete evidence package.

Protect SARs and their existence against unauthorised disclosure. Do not tip off the player or another person. Keep access limited and separate from routine customer-service records. A SAR does not itself authorise confiscation or execution of a suspect transaction. Follow applicable legal restrictions and lawful directions; record the MLRO's decision on continuing, restricting or ending activity.

9.3 Currency transaction reports

For this Code, a CTR is a threshold-based report of completed reportable funds movements in any currency or virtual asset. It is not limited to physical cash and does not require suspicion. Submit a CTR where a single reportable transaction, or linked reportable transactions in either direction, equals or exceeds US \$10,000 or equivalent, applying the procedure on the following page.

SAR and CTR obligations operate independently. Where both apply, submit both and cross-reference them securely. Do not mark a CTR as suspicious unless the facts warrant a SAR.

9 CTR calculation and submission procedure

9.3.1 Reportable movements and gross calculation

Include settled deposits and other external funding, withdrawals, external refunds or payouts, and permitted transfers between different players. Calculate incoming and outgoing amounts separately on a gross basis. Do not offset either direction against the other; do not add incoming and outgoing amounts together to create the threshold. Include fees debited from the player in the gross instructed outgoing amount and record the net amount delivered separately.

Exclude ordinary wagers, settlement of winnings within the same player's gaming balance, non-withdrawable bonuses, transfers between the same player's internal accounts, failed payments and genuine corrections with no funds movement. Record and monitor them under Articles 8 and 9.1. An external refund is an outgoing movement, not a deduction from an earlier incoming movement. Count each funds movement once per direction; internal ledger entries must not duplicate it.

9.3.2 Linked activity and aggregation

Aggregate by player using registration identifiers and available linkage evidence, updating links following verification, across accounts, brands, currencies and payment methods under the same licensee. At each FATF Standards informed edition | Page 6

settled transaction, assess the rolling 24-hour period ending at that timestamp, including both endpoints. Aggregate different players where documented evidence gives reasonable grounds to identify common beneficial control or a coordinated series. A common IP address, device or payment instrument is an indicator requiring assessment, not conclusive evidence on its own.

Where transactions outside 24 hours are demonstrably parts of one planned or coordinated funds movement, aggregate that complete series regardless of duration and report when its cumulative incoming or outgoing value reaches the threshold. Record the evidence, start date and constituent transactions. Mere repeat activity by one player over their lifetime does not itself create an indefinitely linked series. Investigate possible structuring and file a SAR when warranted.

9.3.3 Currency and virtual asset valuation

For CTR purposes, convert each movement into USD at settlement time. For Article 6 KYC calculations, apply the same methodology using EUR. For fiat currency, use the actual documented USD conversion rate where conversion occurs; otherwise use a consistently applied independent market-data source at that time. For virtual assets, use a documented liquid-market USD spot price at settlement time, including for stablecoins. Do not assume perpetual one-to-one parity. Document fallbacks for unavailable or unreliable prices and preserve source, time, units, rate and calculation. Do not revalue historical movements at the reporting date.

9.3.4 Reporting cycle and repeat reports

The weekly reporting period is Monday 00:00 UTC to the following Monday 00:00 UTC, excluding the ending timestamp. File by 17:00 UTC on the following Tuesday, regardless of local holidays. Attribute a report to the period in which a threshold is first met or a new qualifying movement or linked-series extension occurs. Include preceding-period transactions where needed to explain the threshold. Submit a nil return where no qualifying activity occurred.

Where qualifying activity or linkage is identified retrospectively, file promptly and no later than the Tuesday deadline for the reporting week in which it is identified. State original transaction dates, discovery time, affected periods and reasons for delayed identification; amend affected earlier reports where needed. This rule does not excuse avoidable monitoring failures or delay a SAR.

Use one CTR case per player or linked group and direction for each reporting week, with all qualifying windows and constituent movements. Consolidate overlapping windows and identify each transaction once in that week's detail. Previously reported movements may appear as marked context in a later qualifying window. New qualifying activity requires a new weekly CTR, cross-referenced to earlier cases; a continuing linked series requires a supplementary report in each week with new series activity. Correct errors by amendment, preserving the original and its reference.

9 CTR filing requirements and examples

9.3.5 Required data and evidence

Use the dedicated CTR structure in Annex A through the secure channel specified in the adoption notice. The notice must identify a functioning primary and contingency submission route before these provisions commence. Ordinary unsecured email is not an approved transmission route for identity documents or reporting files.

Attach a transaction schedule, USD valuation evidence and, for multi-person groups or series extending beyond 24 hours, a short linkage explanation. Identity documents and full source-of-funds files must be securely retained and supplied on request, rather than routinely attached to every non-suspicious CTR. The

regulator may require additional evidence. An incomplete identity record must not delay a CTR; report available information and update it under Annex A. Retain the receipt and resolve delivery failures immediately using the designated contingency route; a technical failure does not cancel the reporting obligation.

9.3.6 Worked examples

- A settled incoming payment of exactly US \$10,000 triggers a CTR. Incoming and outgoing payments of US \$6,000 each do not create a combined US \$12,000 threshold. Apply the separate EUR 3,000 KYC and withdrawal-request rules before accepting or processing activity.
- Incoming payments of US \$6,000 and US \$4,500 by the same player within a rolling 24-hour period trigger an incoming CTR, including across accounts and currencies.
- Incoming payments of US \$6,000 on Sunday and US \$4,500 on Monday within 24 hours trigger a CTR for the week containing Monday. Include the Sunday payment as threshold context.
- Payments of US \$3,500 in each of three weeks do not automatically trigger CTR aggregation. Evidence that they form one planned US \$10,500 series requires a CTR when the third payment completes the threshold. Apply KYC independently using the historical EUR equivalent of deposits and the other Article 6.2 triggers.
- A US \$12,000 incoming payment followed by a US \$12,000 withdrawal triggers separate incoming and outgoing CTRs. A SAR is also required where suspicion arises. Required CDD or EDD must be completed before the withdrawal.
- Overlapping 24-hour windows must be detected continuously. Mark previously reported movements as context in later qualifying windows, without representing them as newly settled movements.

10 Internal controls and training

Maintain current written policies covering governance, risk assessments, CDD, EDD, sanctions, PEPs, monitoring, payments, virtual assets, reporting, records and incident response. Implement access controls, dual authorisation for sensitive account changes and an auditable exception process. Reconcile payment and gaming ledgers with the data used for reports.

Train relevant staff before independent duties, at least annually and following material changes. Tailor training to onboarding, payments, VIP, customer-service, technical and management roles. Include red flags, escalation, confidentiality, deadlines and reporting examples. Assess understanding and retain participation, results and remedial actions.

11 Information security and data protection

Apply proportionate safeguards for identity evidence, financial records and reports, including access restriction, multifactor authentication, encryption, secure transfer, logging, backups and recovery testing. Limit collection, use and sharing to lawful purposes. Assess vendors and cross-border transfers under applicable data-protection law.

Notify the designated regulatory incident channel within 24 hours after discovery of a material cybersecurity incident affecting player data, funds, AML controls or reporting. Provide an initial account of known facts, impact and containment, followed by updates. Meet any shorter legal notification period and other licence-condition obligations. Reporting an incident does not replace a SAR where suspicious financial activity is present.

12 Independent assurance and regulatory access

Arrange an independent AML/CFT audit at least annually by a competent person or function independent of the operations tested. Scope must cover actual control effectiveness, risk assessment, onboarding, payments, sanctions, PEPs, virtual assets, data quality, SARs, CTRs, record keeping and staff competence. Test samples and systems; a policy-only review is insufficient.

Give senior management the findings, risk ratings and remediation plan. Assign owners and deadlines, verify closure and report material failures promptly to AOFA. Provide records and access for lawful regulatory inspections and requests, including records held by service providers. Do not conceal relevant deficiencies or obstruct regulatory access.

13 Compliance and enforcement

Maintain an auditable compliance record and cooperate with lawful requests from AOFA, competent financial intelligence and law-enforcement authorities. Preserve relevant evidence when an investigation or dispute is known or reasonably anticipated.

AOFA may take action for non-compliance within its lawful powers, including directions, licence suspension or revocation and other sanctions legally available. Financial penalties and public disclosures require an applicable legal basis and appropriate procedure. The Code does not itself create a new criminal offence or an unlimited power to impose penalties. Serious suspected offences may be referred to competent authorities.

14 Review and implementation

Operators must review the effectiveness of their controls at least annually and following regulatory change, significant incidents, audit findings or new risk information. Technology may assist but does not replace accountable human decisions. Validate automated systems, including AI tools, for accuracy, privacy, bias, explainability and operational resilience.

AOFA's adoption notice must state the approved version, effective date, transitional milestones, report recipients and submission channels. Operators must acknowledge receipt and appoint an implementation owner. Existing obligations continue until the replacement takes effect. Any time-limited implementation relief must be explicit; there is no implied exemption from applicable law, sanctions or SAR duties.

Annex A Dedicated CTR submission structure

This is the minimum CTR data specification. AOFA may publish a form or machine-readable schema containing these fields. Operators must not substitute a SAR form for a routine CTR.

A1 Submission and operator details

- Report type: new CTR, supplementary CTR, amendment or nil return; unique operator report reference; previous report references where applicable.
- Operator legal name, licence number, covered brands, MLRO name and secure contact details.
- Reporting period in UTC; date and time of filing; incoming or outgoing direction; single transaction, rolling-window aggregation or extended linked series.

A2 Player and linkage details

- Legal name, date of birth, residential country and address to the extent known; unique player and account identifiers; identity verification status, date and method; risk rating and EDD status. Mark each item as verified, unverified, unavailable or pending where appropriate and explain material gaps.
- For linked groups: details for each participant, controlling person where known, shared identifiers, the evidence of common control or coordination, and the basis for aggregation.
- For extended series: case identifier, start date, nature of the common purpose, cumulative value and reference to the initial report.

A3 Transaction schedule

- Unique transaction identifier; UTC settlement time; brand and player account; transaction category; direction; status; gross original amount; currency or asset; gross USD equivalent.
- Rate, rate source and valuation timestamp; fees and net amount where relevant; payer and payee identifiers; payment provider; appropriately protected instrument references.
- For virtual assets: network, transaction hash and relevant wallet addresses.
- Threshold-triggering transaction and relevant window boundaries; qualifying subtotal; series cumulative total where applicable; clearly marked previously reported context; references to refunds or corrections.

A4 Review and attachments

- Short explanation of the threshold and linkage; related CTR references; restricted SAR reference where applicable and permitted.
- Transaction schedule, valuation evidence and linkage explanation when required; list of additional records retained and available on request.
- MLRO or authorised compliance reviewer confirmation that the report is accurate to the best of their knowledge; date of approval; filing receipt.

File CTRs on time with available information despite incomplete identity checks. Identify gaps and restrictions, then amend or supplement promptly when material information arrives. Reporting does not permit activity restricted pending verification. Threshold activity alone is not suspicion; where suspicion arises, file a separate SAR and protect cross-references.