

Know Your Customer (KYC) Policy

Company: Turn 1 B.V. (operating as New Wave Poker)

MLRO: Dawod Dawood

Version: Draft v2.1

Last Reviewed: September 8th 2025

Next Review: Prior to go-live

Distribution: All relevant staff; regulatory authorities upon request

Draft & Site-Status Notice

Turn 1 B.V. has set the site to “Coming Soon” and is not accepting customers or transactions at this time. This policy is submitted to the Curaçao Gaming Control Board as a draft to evidence our intended control framework. Final operating procedures (including workflow screenshots, staff R&Rs, and system controls) will be completed and trained prior to launch and updated to reflect any supervisory feedback.

1. Purpose and Scope

This KYC policy sets the framework for identity verification, player management (risk-based CDD, monitoring), and the suspension/closure of player accounts for Turn 1 B.V., referencing Curaçao’s AML/CFT regime (NOIS/NO RUT), sanctions legislation, and supervisory guidance, as administered by the Curaçao Gaming Control Board—designated as the Curaçao Gaming Authority under the new framework.

2. Legal & Regulatory Alignment

We align with:

- NOIS / LID (National Ordinance on Identification of Clients when Rendering Services) and NORUT / LMOT (National Ordinance on the Reporting of Unusual Transactions), as amended; applicable sanctions ordinances; and FATF/CFATF expectations.
- GCB/CGA regulations and guidance for land-based and online casinos, including the NAF 4,000 threshold for CDD, linked transactions treatment, timing of verification, and unusual-transaction reporting obligations.

Internal policies may be stricter than minimum legal requirements where our risk assessment warrants it.

3. Governance and Oversight

MLRO: Dawod Dawood. Responsibilities include policy ownership, training oversight, STR/UTR governance, regulator liaison, and annual reporting.

We will maintain:

- A documented Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) methodology;
- Appointment of a Compliance Officer (independent of operations);
- Ongoing training and an independent audit of AML/KYC controls.

4. Player Identification (Customer Acceptance Policy)

4.1 Registration

At account opening, collect name, permanent residential address, and date of birth; perform age verification (18+), and conduct real-time PEP and sanctions screening before any financial capability is enabled. Ongoing re-screening is performed on a risk-based schedule (daily batch as a minimum) and immediately upon profile changes or sanctions list updates.

4.2 Risk-based early elevation to Full CDD

If risk indicators are present at or immediately after registration (e.g., high-risk geography/VPN, PEP or sanctions hit/close match, adverse media, device anomalies, payment-method risk, or first crypto use), Turn 1 may require full CDD immediately and keep deposits/withdrawals/bonuses/transfers disabled until completed.

4.3 When full CDD is mandatory

- Full CDD is required when the player's daily cumulative financial transactions (deposits, withdrawals, and peer-to-peer transfers) reach NAf 4,000 (or equivalent), or upon first withdrawal.
- If USD2,000 is reached by a deposit: block further deposits and withdrawals; play with existing funds may continue where permitted.
- If USD2,000 is reached by a withdrawal: apply a full account freeze (no play).
- If requested documents are not provided within 30 days where verification is required, the account remains fully restricted and is referred to the MLRO for a closure decision. Player balances are kept segregated and, where no ML/TF or sanctions concerns exist, any legitimate funds are returned to the verified original funding method (return-to-source). If that is not possible, payout may be made only to an alternative method verified in the same name with Compliance approval. Funds linked to suspected ML/TF or sanctions issues are held pending investigation and may be reported to the FIU as required by law.

Operational timing rules:

- If the threshold is hit by a deposit, deposits/withdrawals are blocked until CDD completion (player may continue to play with existing balance).
- If the threshold is hit by a withdrawal, the account is fully frozen until CDD completion.
- If the requested CDD is not provided within 30 days post-threshold, we close the account.

4.4 Account Restrictions

One account per person. No cash transactions. Restricted jurisdictions blocked. Duplicate/fraud-suspect accounts suspended pending review.

5. KYC Documentation Standards

5.1 Applicability

These standards apply to all players and all verification levels. Full CDD must be completed before any first withdrawal and when a player meets the statutory verification trigger (\$2,000 daily cumulative financial transactions or equivalent), or earlier on a risk basis.

5.2 Identity documents (one of)

Acceptable, valid, government-issued photo ID:

- Passport, national ID card, or driver's licence.
- Must show full name, date of birth, photo, document number, issuing authority, and issue/expiry dates (expiry at least 3 months away).
- Images must be full colour, all corners visible, no glare/cropping, unaltered. Where present, MRZ and/or signature should be visible.

5.3 Proof of address (recency alignment)

Document showing the player's full name and current residential address matching the account profile: utility bill (electricity, gas, water, fixed internet), bank/credit card statement, government correspondence, or council/property tax bill. Issued within the last 6 months. Screenshots of online statements are acceptable if issuer, date, name, and address are clearly visible. PO Boxes are not accepted as residential addresses.

5.4 Payment method verification

Cards:

- Clear images of the front and back (or bank-issued digital card view). First 6 and last 4 digits visible only; CVV fully covered; cardholder name visible; card must be in the player's name and valid.

Bank transfer / e-wallets (e.g., Skrill, Neteller):

- Screenshot or statement showing account holder name or email, account identifier, and a transaction to/from Turn 1. Platform/issuer branding should be visible. The account must be in the player's name and verified with the provider.

Name mismatches (e.g., joint accounts) require supporting documents and Compliance approval.

5.5 Cryptocurrency wallets

- Evidence of ownership of the sending wallet (for example, an exchange account profile screenshot showing the player's name or email and the wallet address, or a self-custody wallet screen demonstrating control).
- On-chain transaction reference (hash) linking the player's wallet to Turn 1 provided on request.
- Deposits from mixers/tumblers, privacy-enhanced coins, sanctioned or flagged addresses, or unverifiable P2P sources are not permitted.
- Additional EDD (for example, source of funds/wealth and exchange KYC evidence) may be required for higher-risk crypto activity.

5.6 Liveness, biometrics, and face match

- A selfie/liveness check may be required to confirm the person presenting the ID is the legitimate holder.
- Face matches must meet vendor quality thresholds; discrepancies are escalated for manual review.

5.7 Document quality, authenticity, and translation

- Only clear, high-resolution colour images (JPEG/PNG/PDF) are accepted; scans or photos must be unaltered and complete.
- Edited, filtered, or tampered images are prohibited and may result in rejection and account action.
- Documents not in supported languages may require a certified translation; non-Latin scripts may require transliteration.
- Where authenticity is in doubt, further verification (databases, issuing-authority checks, or video call) may be required.

5.8 Name and address variations

- Minor spelling or transliteration differences may be accepted with supporting evidence (for example, marriage certificate, deed poll, national registry printout).

- If the player has recently moved, additional proof may be requested (for example, tenancy agreement plus a utility bill at the new address).

5.9 Expiry, re-verification, and change management

- ID expiry is monitored; re-verification may be required before expiry or upon material profile changes (name, address, payment method), risk events, or sanctions/PEP status changes.
- Any change to personal details or funding methods may trigger partial or full re-verification.

5.10 Recordkeeping and security

- All KYC records are stored securely with encryption and role-based access controls.
- Records are retained for 5 years after account closure (or longer if required by law) and disposed of securely thereafter.
- An audit trail is maintained for verification decisions, document reviews, and escalations.

5.11 Non-compliance

- Failure to provide acceptable documents within requested timelines may result in account restrictions, suspension, or account closure, and regulatory reporting where applicable.

6. Player Management (Risk-Based CDD & Monitoring)

6.1 Risk methodology (CRA scale and bands)

We assign a player risk rating at onboarding and update it continuously using the Company's Customer Risk Assessment (CRA) scale of 1–18. Initial rating is set at registration and recalculated on material events (deposits/withdrawals, device or geolocation change, payment method change, sanctions list updates, Game Integrity alerts).

Bands

- Low risk: CRA 1–6
- Medium risk: CRA 7–12
- High risk: CRA 13–18

Controls

- Low: standard limits; CDD as described in this policy; routine monitoring
- Medium: reduced limits; earlier SoF/SoW requests; manual withdrawal review

- High: deposit/withdrawal restrictions; mandatory EDD; management approval for limit increases; enhanced monitoring

Primary factors

Geography (FATF/CFATF status, sanctions exposure, IP/geolocation integrity); Identity/KYC (document quality, liveness/face match result, PEP/sanctions/adverse media); Payments (method risk across cards, bank, wallets, crypto; name match; chargebacks; return-to-source feasibility); Behaviour (device fingerprinting, IP sharing, velocity/volumes, play patterns, bonus usage); Product (poker tournament/cash dynamics, P2P transfers, agent/affiliate channel risk).

6.2 KYC/CDD elevation rules (include P2P gating)

We may require full CDD earlier than statutory triggers where risk indicators are present (for example, high-risk geography, VPN/hosting IP, PEP/close match, adverse media, device anomalies, first crypto use, or name mismatches). Until satisfied, deposits, withdrawals, bonuses, and peer-to-peer transfers remain disabled. If the requested documents are not provided within 30 days of request, the account will remain restricted and be referred to the MLRO for a closure decision. If the account is closed, any legitimate funds are returned to the verified original funding method; funds linked to suspected money laundering, terrorist financing, or sanctions issues are held pending investigation and may be reported to the FIU.

6.3 Ongoing monitoring rules

Automated rules generate alerts; analysts review and decide actions. In addition to behavioural and payments monitoring, the system checks for statutory verification triggers.

Financial flow and threshold checks

- Daily cumulative financial transactions (deposits, withdrawals, and peer-to-peer transfers) reaching USD2,000.
- Multiple transactions clustered just below the USD2,000 daily threshold (structuring).
- First withdrawal within 24 hours of first deposit.
- Net withdrawal $\geq 80\%$ of prior 24h deposits with minimal play.
- Fan-in/fan-out patterns on peer-to-peer transfers.

Identity, device, location

Rapid device changes; emulator/jailbroken indicators; multiple accounts per device; IP mismatch with KYC country; TOR/VPN/hosting ASN at login or payment; reused KYC artefacts across accounts.

Cryptocurrency

New wallet after a previous wallet flag; links to mixers or sanctioned/high-risk clusters; multiple small deposits from unrelated addresses followed by a large withdrawal.

Sanctions/PEP/adverse media

Screen at onboarding; daily batch re-screen; immediate re-screen on profile edits and list updates. Escalate hard matches to the MLRO and apply appropriate account restrictions, up to and including a full freeze and potential closure. Legitimate funds are returned to the verified original funding method; funds linked to suspected money laundering, terrorist financing, or sanctions issues are held pending investigation and may be reported to the FIU.

6.4 Poker-specific monitoring

Game Integrity monitoring is performed in collaboration with our external provider, RunGood OÜ. Signals include collusion, chip dumping, bot/RTA suspicion, multi-accounting/stabling, SNG/MTT anomalies (e.g., bubble-time behaviour), cash-game short buy-in cycling, and bonus/rakeback abuse.

Actions

Immediate table removal and temporary account hold for P0/P1 integrity alerts; hand-history and network-graph analysis; HUD-less statistical review where applicable; value-at-risk assessment to determine balance holds, confiscation per T&Cs, and restitution; escalation to the MLRO if ML/TF is suspected; consider FIU reporting where applicable.

6.5 Alert severity, SLAs, and actions

Severity levels

- P0: confirmed or highly likely ML/TF or major integrity threat — full freeze; analyst start within 3 hours; MLRO notified
- P1: strong suspicion or material risk — restricted account; review within 24 hours
- P2: anomaly needing clarification — soft hold or friction; review within 3 business days

Possible actions

- No action; monitor
- Add friction: lower limits, manual withdrawal review, SoF/SoW, method removal
- Partial hold: block deposits/withdrawals; allow play with existing funds (as permitted)
- Full freeze: no play or transactions
- Close the account; return legitimate funds to the verified original funding method (return-to-source); hold any funds linked to suspected money laundering, terrorist financing, or sanctions issues pending investigation; submit an Unusual Transaction Report (UTR) to the FIU where required.

6.6 Escalation and roles

- Game Integrity identifies gameplay-based risks and provides case files (hand histories, network graphs, device/IP link analysis) to Compliance

- Compliance owns CDD/EDD, sanctions/PEP, payments and FIU reporting decisions
- Payments returns funds to verified source only; alternative payout requires Compliance approval
- MLRO approves high-risk decisions (EDD outcomes, terminations, FIU filings)

6.7 Data sources and tooling

We use defined data sources and tools to support identity verification, risk scoring, monitoring, and investigations, and to maintain a reliable audit trail.

Core systems and signals

- KYCAID: document capture and verification, liveness/face match, proof-of-address collection, and (where enabled) sanctions/PEP screening.
- Sanctions/PEP/adverse media screening service: initial screening at registration and ongoing re-screening (may be integrated with KYCAID or operated separately).
- Device intelligence and IP geolocation: device fingerprint, emulator/jailbreak indicators, TOR/VPN/hosting ASN, IP country/region, and device/linkage analytics.
- Payment gateway and banking signals: AVS, 3-D Secure outcomes, chargeback alerts, and (where available) Confirmation of Payee/Open Banking name-match results.
- Blockchain analytics: wallet ownership evidence, address clustering, mixer/tumbler exposure, and sanctions/high-risk address flags.
- Game Integrity analytics (RunGood OÜ): hand histories, gameplay pattern metrics, network-graph/link analysis, and collusion/chip-dumping/bot indicators.
- Case management and alerting: workflow, decisions, timestamps, reviewers, and evidence repository.
- Data warehouse and logs: transactions, sessions, payments, KYC events, and audit logs.

Access and controls

- Access is limited to trained personnel on a least-privilege basis (Compliance/MLRO, Game Integrity, and Payments as relevant).
- All queries and decisions are logged; changes to rules or vendor configurations follow documented change control and are approved by Compliance.
- Third-party providers are under contract with appropriate data-processing terms; security and privacy reviews are performed before onboarding and periodically thereafter.

Operations and quality

- Automated alerts do not determine outcomes without human review; analysts document the rationale and evidence for each decision.
- Thresholds and rules are reviewed monthly using alert performance metrics; tuning is recorded in the change log.
- If a vendor is unavailable, staff use a documented fallback (for example, secure file upload and manual checks) and re-run automated checks when service resumes.

Retention and security

- Artefacts and logs are retained securely for at least five years after account closure, encrypted at rest and in transit, and available for audit on request.

6.8 Model governance and tuning

This section defines how we design, evaluate, and change risk rules and model thresholds used for CDD/EDD, sanctions/PEP screening, device intelligence, cryptocurrency analysis, payment signals, and Game Integrity alerts (including vendor-provided models).

Ownership and decision-making

Compliance owns rule design and tuning; the MLRO is accountable. A monthly governance meeting includes Compliance, Game Integrity, Payments, Data/Analytics, and Security. Decisions are minuted with clear owners and due dates.

Review cadence

- Monthly: review alert performance and propose threshold changes.
- Quarterly: refresh the risk assessment, assess control effectiveness, run scenario tests for new typologies, and sample closed cases for quality.
- Annually: commission an independent audit covering monitoring rules, case management, documentation, and recordkeeping practices.

Performance metrics

Track at minimum: alert precision and recall, false-positive rate, alert volume, time to first action, case closure time, proportion escalated to MLRO, proportion resulting in restrictions/EDD/closure, value-at-risk captured or prevented, and UTR/STR submission rates.

Change management

Every change is raised via a documented request stating rationale, expected impact, and success criteria. Changes are tested in UAT or backtested on recent data, approved by Compliance and the MLRO, scheduled for deployment, and followed by a defined monitoring period with a post-implementation review. Each change includes a rollback plan. A versioned change log and rule inventory are maintained.

Data quality and dependencies

Daily checks confirm sanctions/PEP list freshness, vendor API health, data-feed completeness and timeliness, and clock/time-zone consistency. Any material data issue triggers an operational alert and temporary compensating controls.

Poker-specific tuning

Coordinate monthly with Game Integrity to review collusion/chip-dumping/bot signals, recalibrate thresholds using recent hand histories and network-graph outcomes, and shadow-test new rules before activation to measure impact on false positives and detection lift.

Vendor model management

Record vendor model versions and parameter changes (for example, KYCAID liveness thresholds). Obtain release notes, test material updates in UAT where feasible, document approvals, and track enablement dates in the change log.

6.9 Quality assurance

Objective

Ensure investigations and decisions are correct, timely, well documented, and consistent; identify training needs and improve rules and processes.

Scope

Quality checks apply to all monitoring alerts and investigations across sanctions/PEP, payments, device/location, cryptocurrency, and Game Integrity. Reviews cover both “no issue” closures and actioned cases.

Sampling plan

- At least 10% of closed cases each month, with a floor of 50 where volumes permit.
- Include all P0 cases, at least 50% of P1 cases, and a rotating sample of P2 cases.
- Oversample “no issue” closures to detect potential false negatives.
- Add a small random sample from new reviewers (first 90 days) and any reviewer below target last month.

Review method and rubric

A reviewer who did not own the original case rechecks: decision correctness; investigation depth; evidence quality; timeliness (time to first action and to closure); narrative quality; funds handling; regulatory steps; and data protection.

Metrics and targets

Track monthly: decision accuracy, false-positive rate, time to first action, time to closure, documentation quality, cases reopened, and reviewer pass rates. Material shortfalls trigger corrective actions.

Independence and calibration

QA is performed by staff independent of the original case. A monthly calibration session aligns scoring using recent anonymised cases.

Corrective and preventive actions

Raise actions with an owner, due date, and effectiveness check. Actions may include targeted training, playbook updates, rule/threshold tuning, or tool changes.

Reopen and escalation

If QA finds an incorrect decision or missed risk, reopen the case, apply appropriate restrictions or other actions, and notify the MLRO where warranted. Document changes and notifications in the case record.

Reporting

Publish a monthly QA report to the MLRO and relevant leads summarising metrics, key findings, root causes, and action status.

6.10 Documentation and recordkeeping

Maintain complete, accurate, and retrievable records that evidence how KYC/CDD/EDD, monitoring, decisions, and funds handling were performed.

Scope

- KYC onboarding and re-verification, sanctions/PEP screening, adverse media checks
- Monitoring alerts and investigations across payments, device/location, cryptocurrency, and Game Integrity
- Decisions, approvals, restrictions, freezes, closures, and funds handling
- Communications with players and third parties
- Regulatory submissions and correspondence (for example, FIU reports and regulator queries)

Case file contents (minimum)

- Unique case ID; player identifiers; date/time opened and closed
- Trigger or alert details (rule name/threshold at time of firing)

- Analyst narrative explaining the risk, evidence considered, and rationale for the decision
- Actions taken and dates (e.g., limits applied, holds, freeze, re-verification requested)
- Approvals and by whom (analyst, senior reviewer, MLRO)
- Player and internal communications relevant to the case
- Funds handling record (amounts held/released, return-to-source outcome, alternative method approval if used)
- Regulatory handling (UTR/STR reference, submission timestamp, acknowledgements)
- Evidence list and attachments or links (see “Evidence standards”)

Evidence standards

- Retain source outputs where possible, not just screenshots (for example, vendor PDFs/CSVs, API responses, goAML receipts).
- Examples include: KYCAID verification results and liveness scores; document images as required; sanctions/PEP screening results; payment gateway signals (AVS, 3-D Secure outcomes, chargeback notices); bank statements or Open Banking/Confirmation of Payee results; blockchain analysis notes and transaction hashes; device and IP data at time of event; Game Integrity extracts (relevant hand histories, pattern summaries, linkage graphs).
- Timestamps must be system-generated; where feasible, include file hashes or immutable log references to support integrity.

Storage and security

- Store all records in approved systems with encryption in transit and at rest, and role-based access on a least-privilege basis.
- Access and changes are audit-logged. Exports are limited to operational need and must be watermarked or otherwise controlled.
- KYC documents are collected via KYCAID; email submissions are discouraged and, if received, are moved to the secure repository and deleted from mailboxes.

Retention and disposal

- Retain records for at least five years after account closure, or longer if required by law or regulator instruction.
- Dispose of records securely at end of retention, with a verifiable destruction log.
- Backups follow the same retention and protection standards.

Access and disclosure

- Provide records promptly to the MLRO, internal audit, external auditors, or competent authorities upon lawful request.

- Handle player data in line with data-protection obligations; redact where required by law and avoid any action that could constitute tipping-off.

Time and traceability requirements

- Systems use synchronized time sources; all records show timezone and timestamp precision appropriate to the control (seconds or milliseconds where available).
- Maintain a versioned inventory of active rules at the time of each alert so investigations can be reconstructed accurately.

6.11 Exceptions

Purpose

Allow tightly controlled, time-bound departures from standard controls to address urgent risk or operational failures without weakening the overall framework.

When an exception may be used

- Acute risk requiring immediate action not covered by current rules.
- Temporary vendor or data-feed outage requiring a fallback process.
- Data quality issues that would otherwise block legitimate activity.
- Regulator request requiring bespoke handling.

Authority and approvals

- Planned exceptions require MLRO approval before use.
- Emergency exceptions may be applied by a senior compliance lead with immediate notification to the MLRO and a post-hoc review within five business days.

Documentation requirements (record in the case file and exception log)

- Business justification and risk assessment.
- Scope and controls to be applied in lieu of standard (for example, manual review, temporary limits).
- Start date/time, owner, and the earliest expiry date (“sunset”).
- Approver’s name and date/time of approval.
- Communication plan to affected teams and any player notifications.

Constraints

- Exceptions are time-limited and narrowly scoped; default expiry is 30 days unless renewed by the MLRO.
- They must not contravene law, regulator instructions, or licensing conditions.
- Compensating controls must keep residual risk at an acceptable level.

Monitoring and closure

- While active, monitor the exception's outcomes and capture metrics (volumes affected, incidents avoided, residual risk).
- On expiry or closure, revert to standard controls, document results, and file a brief lessons-learned note.

Governance and reporting

- All active and closed exceptions are reviewed in the monthly governance meeting.
- Recurrent or similar exceptions trigger corrective actions (for example, rule updates, SOP changes, training, vendor changes).
- The exception log is available to internal audit and authorities on request.

6.12 Review cadence (high-risk accounts)

Purpose

Keep risk assessments current and ensure controls match the player's risk profile.

Cadence

- High risk (CRA 13–18): reviewed at least every 30 days.
- Medium risk (CRA 7–12): reviewed at least every 90 days.
- Low risk (CRA 1–6): reviewed at least annually.
- Event-driven reviews: performed immediately when a material risk event occurs.

Event-driven triggers

- PEP or sanctions hard/close match, or adverse media hit
- First withdrawal; daily cumulative financial transactions reaching NAf 4,000 (or equivalent)
- New or changed funding method, name mismatch, chargeback or payment dispute
- Device/emulator indicators, IP/geolocation anomalies, VPN/hosting ASN
- Cryptocurrency wallet change, mixer/sanction exposure flags
- Game Integrity alert (e.g., suspected collusion, chip dumping, bot/RTA)

Scope of each review

- Recalculate CRA score and confirm the correct risk band
- Recheck sanctions/PEP/adverse media status and any open KYC/EDD items
- Analyse recent transactions, gameplay, and device/IP history
- Confirm limits, holds, and monitoring rules are appropriate; adjust if needed
- Decide on any source-of-funds/wealth requests or other follow-ups
- Document rationale, actions taken, next review date, and reviewer

Timeliness and handling

- Start reviews by the due date and complete them as soon as practicable; overdue high-risk reviews are prioritised.
- While a high-risk review is overdue or in progress, withdrawals are subject to manual review.

Governance

- A weekly report highlights upcoming and overdue reviews.
 - Completion rates and key outcomes are reported monthly to the MLRO.
-

7. Enhanced Due Diligence (EDD)

EDD applies when a player presents higher-than-normal ML/TF risk. It supplements standard due diligence with deeper checks, tighter controls, and senior approval.

Triggers — examples include:

- Politically Exposed Person (PEP) or close associate/family member
- High-risk or sanctioned geography indicators (residence, IP, payment origin)
- Cryptocurrency used as a primary or higher-risk funding method
- Player-to-player transfer activity that is material or unusual (for example, cumulative transfers above 1,000 in base currency, circular flows, rapid transfer-withdrawal sequences)
- Red flags from monitoring or Game Integrity review (collusion, chip dumping, multi-accounting, bot/RTA suspicion)
- Anonymity-facilitating products, new/untested delivery mechanisms, or complex payment structures
- Unclear or inconsistent source of funds or source of wealth
- Adverse media or sanctions close match that requires resolution

Measures applied — examples include:

- Source of funds (SoF) and source of wealth (SoW) evidence
 - Payment-method ownership re-verification (gateway/banking signals or provider evidence)
 - Cryptocurrency checks (wallet ownership, on-chain analysis, mixer/sanction screening)
 - Identity reinforcement (repeat liveness/face match, secondary ID, video call)
 - Senior review by the MLRO or designated compliance lead
 - Enhanced monitoring (lower thresholds, manual withdrawal approval)
-

8. KYC/Verification Process

8.1 Third-party verification (KYCAID)

- The platform generates a unique, time-limited KYCAID link and logs the event.
- The link is sent via Zendesk macro with instructions not to email documents; if documents are emailed, support redirects the player to the KYCAID link.
- KYCAID performs document capture and automated checks (ID OCR, liveness/face match, proof of address, and—where enabled—sanctions/PEP screening).
- Results are returned to the Turn 1 dashboard/webhook and to the designated compliance inbox (kycaid@newwavepoker.com).
- Account status is updated automatically:
 - Verified: permitted capabilities are enabled subject to risk controls.
 - Action required: additional evidence requested; deposits, withdrawals, bonuses, and P2P transfers remain restricted.
 - Failed/suspected fraud: account is frozen and escalated to Compliance.
- Reminder cadence for outstanding requests: send reminders around day 3, 7, 14, and 28. If requested documents are not provided within 30 days, the account remains restricted and may be closed by the MLRO. Legitimate funds are returned to the verified original funding method; funds linked to suspected money laundering, terrorist financing, or sanctions issues are held pending investigation and may be reported to the FIU.
- KYCAID supports payment-method evidence capture (masked card images, e-wallet or bank screenshots, crypto wallet ownership evidence) consistent with the documentation standards in this policy.

8.2 Manual review

- Senior compliance staff review flagged or high-risk cases, resolve close matches, and perform cross-checks (document authenticity, face match quality, identity data consistency, payment-method ownership, and—where relevant—on-chain analysis for crypto).
- Outcomes: approve; request additional information; reject; offboard; or escalate to the MLRO.
- Service levels: standard KYC reviews are targeted within one business day; urgent cases with pending withdrawals or threshold triggers are prioritised same-day.
- Two-person review is used for high-risk decisions and negative outcomes where practicable.
- Every decision includes a clear analyst narrative, evidence list, timestamps, and the reviewer's initials.

8.3 Quality assurance for verification

- Sample a proportion of passed, failed, and “action required” KYC cases each month to assess decision correctness, investigation depth, evidence quality, turnaround time, and narrative clarity.
- Track reviewer error rates and turnaround times; provide targeted training where needed.
- Update fraud patterns and playbooks when recurring issues are identified.
- Include verification in the scope of independent audit.

8.4 Fallback and continuity

- If KYCAID is unavailable, use a secure alternative (for example, one-time secure upload) to collect equivalent evidence.
- Once service resumes, migrate the artefacts into KYCAID or the case system so the audit trail is complete and consistent.

8.5 Accessibility and vulnerable customers

- Provide reasonable alternatives if a player cannot use the standard capture flow (for example, assisted video verification or additional time to respond).
- Balance accommodations with risk; apply temporary restrictions where appropriate until verification is complete.

8.6 Player communications

- Communications are clear and neutral. Rejection reasons are stated at a high level (for example, unreadable image, expired document, name/address mismatch) without disclosing sensitive detection methods.
- All communications related to verification are logged to the case record.

9. Suspension and Closure of Player Accounts

9.1 Temporary suspension

Grounds include pending CDD/EDD or re-verification, sanctions/PEP matches or close matches, unusual or rapid transaction patterns, device/IP anomalies, suspected account takeover, Game Integrity alerts (e.g., collusion, chip dumping, bot/RTA), payment-method anomalies, regulatory checks, self-exclusion, or other security concerns.

Actions may include restricting deposits, withdrawals, bonuses, and peer-to-peer transfers, removing table access, and requesting additional information.

Notify the player within 24 hours where lawful and appropriate. Communications are neutral and avoid tipping-off. A review is initiated promptly (P0 within 3 hours; P1 within 24 hours; P2 within 3 business days).

9.2 Permanent closure

Grounds include failed or fraudulent KYC/EDD, underage gambling, multiple accounts, confirmed money laundering/terrorist financing or fraud, sanctions match, prohibited jurisdictions or VPN/hosting misuse, integrity violations (e.g., collusion, chip dumping, bot/RTA) consistent with Terms and Conditions, non-cooperation with required checks, serious abuse, or regulator instruction.

Closures are approved by the MLRO or a designated senior compliance officer. Where the basis is gameplay integrity, Compliance and Game Integrity agree the decision; a two-person review is used where practicable.

9.3 Process and timelines

- When the daily cumulative financial-transaction threshold of USD2,000 is reached by a deposit: block further deposits and withdrawals; the player may continue to play with existing funds unless other risks are present; request verification documents and start a 30-day clock.
- When the threshold is reached by a withdrawal: apply a full account freeze; request verification documents and start a 30-day clock.
- For sanctions/PEP hard matches, confirmed fraud, or account takeover: apply a full freeze immediately.
- Send reminders for outstanding documents around day 3, 7, 14, and 28. If documents are not provided within 30 days where verification is required, keep the account restricted and refer to the MLRO for a closure decision.
- Player notifications state the status and what is required, without disclosing sensitive detection methods. All actions, evidence, and decisions are recorded in the case file.

9.4 Funds during suspension or closure

Player balances are kept segregated from operational funds. Where no ML/TF or sanctions concerns exist, legitimate funds are returned to the verified original funding method (return-to-source). If that is not possible, payout may be made only to an alternative method verified in the same name with Compliance approval.

Funds linked to suspected money laundering, terrorist financing, sanctions issues, confirmed fraud, or unresolved integrity violations may be held pending investigation and reported to the FIU where required. For gameplay-integrity closures, balances may be adjusted or forfeited in line with the Terms and Conditions (for example, confiscation of unfair winnings and restitution to affected players), with full documentation.

Any lawful set-off (e.g., chargebacks, unpaid fees) is applied only where permitted by law and licence conditions. Unclaimed or abandoned balances are handled in accordance with applicable law.

10. Suspicious Activity & Reporting (UTR/STR)

10.1 Purpose and scope

Set out how staff identify, escalate, and report unusual/suspicious activity and how the MLRO files Unusual Transaction Reports (UTRs) to FIU Curaçao via goAML.

10.2 Definitions and indicators

- Unusual/suspicious activity: transactions or behaviours that meet objective indicators published by the FIU or for which there are reasonable grounds to suspect money laundering or terrorist financing.
- Indicators (examples include): profile mismatches; reluctance to provide KYC; rapid deposit–withdrawal with minimal play; structuring just below verification or reporting thresholds; multiple funding methods without clear purpose; device/IP anomalies (VPN/TOR/hosting ASN); use of high-risk payment channels; crypto flows linked to mixers/sanctioned clusters; player-to-player value transfer patterns; Game Integrity red flags (collusion, chip dumping, bot/RTA); adverse media; sanctions/PEP hard or close matches.

10.3 Staff duties on suspicion

- Stop or delay the affected transaction where lawful and feasible without tipping-off.
- Escalate immediately to Compliance via the designated channel and mark urgency (P0/P1/P2).
- Do not inform the player or third parties that a report may be filed.
- Preserve evidence: screenshots, logs, device and IP data, payment signals, KYCAID outputs, hand histories, and any communications.

10.4 Escalation workflow and timelines

- Triage: P0 within 3 hours; P1 within 24 hours; P2 within 3 business days.
- Outcome options: no issue (document and close), monitor, apply restrictions/holds, request information, or prepare a UTR.
- Filing standard: where suspicion remains, the MLRO (or delegate) files a UTR to FIU Curaçao via goAML without delay. Internal target is within one business day of concluding suspicion.
- Apply appropriate account measures in parallel (for example, partial hold, full freeze, method removal), balancing risk and legal constraints.

10.5 UTR content (minimum)

- Player identifiers and current CRA risk band; brief KYC summary.
- Transaction details: date/time, amount, currency, method, counterparties; for crypto, wallet addresses and hashes.
- Narrative explaining the suspicion, relevant indicators, and how it was detected.
- Funds status: held, returned to source, or other disposition.
- Linked accounts, devices, IPs, and any affiliate/agent connections.
- Attachments: key evidence (logs, screenshots, vendor reports).
- Internal reference number and preparer/reviewer details.

10.6 Post-filing handling

- Maintain confidentiality; do not disclose filing to the player.
- Monitor the account and related accounts; file supplemental reports if new material information arises.
- Respond promptly to FIU requests; log all correspondence.
- Do not release funds that are subject to legal or regulatory holds.

10.7 Recordkeeping

- Keep copies of filed/not-filed assessments, UTRs, narratives, evidence, acknowledgements, and correspondence in the case system.
- Retain records securely for at least five years after account closure; ensure encryption, access controls, and an audit trail of who accessed what and when.

10.8 Roles and access

- The MLRO approves all UTR filings; a designated deputy may act in the MLRO's absence.
- Compliance analysts prepare files; Payments and Game Integrity provide supporting data and implement account measures.
- Access to the goAML portal is limited to the MLRO and named delegates with multi-factor authentication.

10.9 Quality and training

- Monthly sampling of both filed and not-filed cases to check decision quality and timeliness; feedback into training and rule tuning.
- Conduct periodic scenario exercises (table-tops) covering UTR drafting, tipping-off avoidance, funds handling, and regulator queries.

10.10 Law-enforcement and regulator requests

Verify the requester's identity and legal basis; log the request; provide only the minimum necessary information; track fulfilment and any onward restrictions or instructions.

11. Data Protection & Confidentiality

11.1 Purpose

Protect player and staff data, meet legal/licensing obligations, and provide complete, auditable records without exposing personal information unnecessarily.

11.2 Scope

All personal data processed by Turn 1, including KYC documents and selfies, sanctions/PEP results, payment method evidence, device/IP data, gameplay logs, investigations, and communications. Applies to employees, contractors, and approved third parties.

11.3 Principles

- Lawfulness, fairness, transparency
- Purpose limitation (use only for onboarding, risk, security, compliance, customer support)
- Data minimisation (collect the least amount needed to achieve the purpose)
- Accuracy (keep data current; correct errors promptly)
- Storage limitation (keep only as long as required)
- Integrity and confidentiality (security by design and by default)
- Accountability (be able to demonstrate compliance)

11.4 Collection and minimisation

- Collect only defined KYC attributes and verification artefacts; avoid free-text personal data where templates exist.
- Redirect players to KYCAID for document capture; discourage email attachments. If received by email, move to the secure repository and delete from mailboxes.
- Use pseudonymised identifiers for analytics and model tuning wherever practical.

11.5 Storage and access control

- Store all records in approved systems with encryption at rest and in transit.
- Apply role-based access on a least-privilege basis (Compliance/MLRO, Game Integrity, Payments, Support as relevant).
- Enforce multi-factor authentication for privileged users and vendor consoles.
- Log all access and changes with timestamp, user, and action; review access logs regularly.
- Protect secrets (API keys, certificates) in an approved secrets manager.

11.6 Transmission and handling

- Use secure channels (TLS) and approved file-transfer methods; do not send KYC documents over unsecured channels.
- Watermark or otherwise control exports; restrict local downloads to operational necessity.
- Prohibit staff from forwarding personal data to personal accounts or devices.

11.7 Third-party processors and vendors

- Use written contracts with data-processing terms, confidentiality, breach notification, and audit rights.
- Vendors include, for example, KYCAID (identity verification) and RunGood OÜ (game integrity analytics).
- Perform security/privacy due diligence before onboarding and at least annually thereafter; document results and remedial actions.

11.8 International transfers

- Where data is transferred cross-border, use lawful transfer mechanisms (for example, Standard Contractual Clauses) and apply additional safeguards based on risk.
- Maintain a register of data locations and transfer bases for each vendor.

11.9 DPIA and change control

- Conduct a Data Protection Impact Assessment for new high-risk processing (e.g., new biometrics, new analytics, new data sharing) or material changes.
- Record decisions, mitigations, and approvals; implement “security by default” in new features.

11.10 Data subject rights

- Provide clear privacy notices explaining what is collected, why, and retention periods.
- Handle access, rectification, objection/restriction, portability, and deletion requests within legal timeframes.
- Verify identity before fulfilling requests; redact third-party data and protect investigation integrity.

11.11 Retention and disposal

- Retain KYC, monitoring, investigation, and reporting records for at least five years after account closure, or longer if required by law or regulator instruction.
- Apply the same protection to backups.
- Dispose of data securely at the end of retention and keep a destruction log.

11.12 Incident and breach management

- Treat any loss, unauthorised access, or misuse of personal data as a security incident.
- Contain, investigate, document, and notify in line with legal requirements and contractual obligations.
- Maintain evidence for audit; avoid tipping-off in AML-related cases.

11.13 Confidentiality and staff obligations

- All staff sign confidentiality commitments and complete privacy/security training at onboarding and annually.
- Access is revoked promptly on role change or exit; devices are returned or securely wiped.
- Disciplinary action may follow any misuse or negligent handling of personal data.

11.14 Monitoring and assurance

- Run periodic access reviews, vendor reviews, and security tests; remediate findings.
 - Include data-protection controls in internal QA and independent audits.
 - Keep policies and procedures up to date and communicate changes to relevant teams.
-

12. Training & Competency

12.1 Purpose

Ensure all relevant staff are trained and competent to prevent money laundering and terrorist financing, apply KYC/CDD/EDD correctly, protect data, and operate monitoring and reporting controls.

12.2 Scope and audience

Applies to all employees and contractors with access to player data or systems, including Support, Payments, Compliance/MLRO team, Game Integrity, Product/Engineering, Marketing/CRM, and Senior Management.

12.3 Frequency and timelines

- Induction: complete core AML/KYC training before system access and within 14 days of start.
- Annual refresher: complete within 12 months of the last certification.
- High-risk roles (Compliance/MLRO delegates, Payments, Game Integrity): refresher every 6 months.

- Event-driven updates: complete targeted micro-training within 30 days of material regulatory or product changes.

12.4 Core curriculum (all staff)

- AML/CTF fundamentals, obligations, and personal liability
- Risk-based approach; player lifecycle; KYC/CDD/EDD basics
- Sanctions/PEP screening and tipping-off avoidance
- Suspicious/unusual activity indicators and escalation workflow
- goAML/UTR concept and internal reporting pathway
- Data protection, confidentiality, and secure handling of KYC documents
- Responsible gaming and vulnerable customer awareness
- Company policies, acceptable use, and disciplinary consequences

12.5 Role-specific modules

Support: identity checks in support flows; secure comms; red flags and escalations.

Payments: return-to-source, name-match signals, chargebacks, method ownership checks.

Compliance/MLRO: case handling, SoF/SoW standards, sanctions/PEP resolution, UTR drafting, funds handling decisions.

Game Integrity: collusion/chip-dumping/bot indicators, value-transfer analysis, evidence packs.

Product/Engineering: logging and audit trails, access controls, data minimisation, control changes.

Marketing/CRM: segmentation and eligibility (no bonuses for restricted accounts), compliant comms.

Senior Management: oversight duties, resourcing, governance, and sign-off responsibilities.

12.6 Tools training

- KYCAID console use (document capture, liveness/face match, decisions, audit exports).
- Screening tool or KYCAID-integrated lists (querying, resolving hits, maintaining evidence).
- Case management system (alert workflow, narratives, evidence linking, approvals).
- Blockchain analytics (where relevant): wallet ownership signals, exposure checks, report exports.
- Game Integrity tooling: hand histories, network graphs, case packaging.

12.7 Methods and delivery

Blend e-learning, live workshops, tabletop exercises, and supervised case shadowing. Use real (anonymised) cases for scenario practice. Provide written playbooks and quick-reference guides.

12.8 Competency assessment

- Passing score: 80% or higher on graded assessments.
- Two attempts permitted; failures require remedial coaching and re-test.
- For high-risk roles, add practical assessments (case write-ups, tool walk-throughs).
- Access to high-risk functions may be limited until the individual is certified.

12.9 On-the-job validation

New Compliance and Game Integrity analysts complete supervised case work until sign-off by a senior reviewer. Early decisions are sampled at an elevated rate for 90 days.

12.10 Records

Maintain training records for each person: modules completed, dates, scores, trainer/assessor, and any remedial actions. Retain records securely for at least five years after employment or contract end.

12.11 Governance and reporting

Compliance owns the program; the MLRO is accountable. Monthly reports show completion rates, overdue items, assessment results, and key findings from QA and audits. Material gaps trigger corrective actions.

12.12 Quality and improvement

Review curriculum annually and after significant incidents or audit findings. Update content for new typologies, product features, vendor changes, or regulatory updates. Collect feedback after each session and track effectiveness using QA outcomes and error-rate trends.

12.13 Non-compliance

Failure to complete mandatory training on time may lead to suspension of system access or duties and, if persistent, disciplinary action.

12.14 Accessibility and localisation

Provide reasonable accommodations (e.g., extended time, alternative formats) and localised content where needed. Ensure materials are clear, concise, and free of unnecessary jargon.

13. Policy Maintenance

13.1 Purpose

Keep this policy current with law, licensing conditions, supervisory guidance, and our operating model; ensure changes are controlled, documented, and communicated.

13.2 Ownership and accountability

Compliance owns this policy; the MLRO is accountable for its accuracy and effectiveness. Senior Management approves material changes.

13.3 Review cadence

- Annual comprehensive review of the full policy.
- Quarterly regulatory check for updates to Curaçao requirements, FIU guidance, and licensing conditions.
- Monthly procedural review to align SOPs and playbooks with the policy.
- Pre-launch checkpoint before accepting customers and after any major product change.

13.4 Triggers for immediate update

Regulatory or supervisory instruction; changes to sanctions regimes; new or amended products, payment methods, jurisdictions, vendors, or monitoring capabilities; material audit/QA findings; incident post-mortems.

13.5 Regulatory monitoring

Track and assess updates from the Curaçao supervisor and FIU Curaçao, relevant sanctions authorities, and FATF/CFATF. Where risk or obligations change, update controls and documentation without delay.

13.6 Change classification

- Material change: alters obligations, player impact, or core controls. Requires Senior Management approval and staff training before effective date.
- Minor change: clarifications or housekeeping with no control impact. Approved by Compliance; notify affected teams.

13.7 Change control and records

Maintain a versioned change log with version number, summary, rationale, impact assessment, approver, effective date, and any required training or system updates. Archive superseded versions; make the current version easily accessible to staff.

13.8 Communication and training

Notify affected teams of changes and provide targeted training where needed. Confirm completion and capture attestations for material changes.

13.9 Document control

Each release shows version, last review date, policy owner, approver, and next scheduled review. External copies provided to authorities match the internal approved version.

14. Go-Live Readiness (to be completed before launch)

Prior to accepting customers, we will:

1. Finalize SOPs (with UI steps), RACI, and evidencing artefacts;
 2. Complete staff training (incl. assessments) and portal registrations (e.g., FIU goAML);
 3. Validate automated monitoring and thresholds in UAT;
 4. Run table-top exercises for UTR/STR, account freezes, and 30-day terminations;
 5. File any updated policy revisions requested by the GCB/CGA.
-

15. Final Statement

Turn 1 B.V. enforces a zero-tolerance approach to ML/TF. We will operate a risk-based KYC/CDD programme, perform ongoing monitoring, and suspend/close accounts where required to protect players, our platform, and the integrity of Curaçao's licensing regime.

Policy Owner: Dawod Dawood, MLRO