Anti-Money Laundering and Counter-Terrorism Financing Policy
TURN 1

Note on Status of Policy
This Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy is a working document. It has been prepared in advance of the Company's full AML/CFT operations and will be revised and expanded as those operations are established. Updates will be made as processes, systems, and controls are implemented and refined.

Effective Date: April 10th 2025
Approved by: Board of Directors
Version: 1.1

Document Control

Version	Date	Description	Author	Approved By
1.1	April 10th 2025	First Regulatory Version	Clodagh Keogh Hansen	Claire Godschalk

Table of Contents

Introduction and Scope

This Policy sets out Turn 1's framework for preventing money laundering and terrorist financing, in line with the Curaçao Gaming Control Board's (GCB) AML- CFT Regulations (January 2025), the National Ordinances (NOIS, NORUT), FATF Recommendations, and global best practices.

This Policy applies to:

- All Turn 1 entities and operations

- Employees, officers, directors
- Contractors, consultants, third-party service providers
- Game Integrity vendors RunGood OÜand KYCAID partners

Definitions

See Appendix A.

Legal and Regulatory Framework

Turn 1 complies with:

- National Ordinance on the Identification of Clients (NOIS)
- National Ordinance on Reporting of Unusual Transactions (NORUT)
- National Ordinance on Games of Chance (NOGC)
- Curaçao AML-CFT Regulations (2025)
- International Sanctions from UN, EU, UK, US OFAC, AU

Governance and Internal Responsibilities

Money Laundering Reporting Officer (MLRO): Dawod Dawood
The MLRO is the central figure in Turn 1's AML/CTF framework and is responsible for:

- Ensuring compliance with AML/CTF legislation and the Curaçao AML-CFT Regulations
- Receiving, reviewing, and submitting Suspicious Transaction Reports (STRs) to the FIU Curaçao
- Maintaining the internal STR register and ensuring timely escalation of red flags
- Approving Enhanced Due Diligence (EDD) measures for high-risk customers
- Liaising with the Gaming Control Board (GCB) and other competent authorities

- Overseeing implementation of the Business Risk Assessment (BRA) and Customer Risk Assessment (CRA)

- Reviewing and signing off on all policy updates and internal audit findings

Compliance Officer: Clodagh Keogh Hansen
The Compliance Officer reports to the MLRO and supports implementation and oversight. Responsibilities include:

- Ensuring proper onboarding of customers in line with CDD/EDD requirements

- Verifying the effectiveness of KYCAID identity verification and sanction screening processes

- Monitoring and testing the operation of internal controls related to AML

- Maintaining AML training logs and coordinating delivery of annual and onboarding training

- Assisting in the preparation of internal audit materials and regulatory reports

- Ensuring timely data retention, policy documentation, and vendor compliance reviews

Board of Directors
The Board holds ultimate accountability for AML/CTF compliance and must:

- Approve the AML/CTF Policy and any subsequent revisions

- Review audit findings and ensure remediation plans are executed

- Ensure the MLRO has sufficient independence, authority, and resources

RunGood OÜ: External. Monitors transaction behavior, collusion, fraud risk, and linked accounts.

Risk-Based Approach (RBA)

Turn 1 applies a Risk-Based Approach (RBA) across its entire AML/CTF program, in line with FATF Recommendation 1 and Curaçao AML-CFT Regulations.

This means resources and controls are focused on areas with the greatest ML/TF risk exposure.

The RBA is implemented through:

1. **Business Risk Assessment (BRA):**
   Conducted annually and approved by the Board, the BRA evaluates inherent risks across Turn 1's business lines, products, delivery channels, payment methods, geographic exposure, and third-party dependencies. (See Business Risk Assessment Section and Appendix C)

2. **Customer Risk Assessment (CRA):**
   Each customer is assigned a risk rating (Low, Medium, High) based on jurisdiction, payment method, product usage, SOF/SOW clarity, and behavioral patterns. The CRA score determines the level of due diligence applied. (See CRA Section and Appendix B)

3. **Risk-Based Controls:**

   - **CDD/EDD Thresholds:** Higher-risk customers are subject to enhanced due diligence, including source of funds verification and senior approval.

   - **Transaction Monitoring:** High-risk customers are monitored with greater frequency and lower tolerance thresholds.

   - **Product Controls:** Peer-to-peer poker, crypto funding, and player transfers are subject to tailored monitoring rules and transfer limits.

4. **Ongoing Risk Review:**
   Customer risk ratings are re-evaluated upon any trigger event (e.g., withdrawal request, large deposit, sanctions hit), and at regular intervals as risk dictates.

5. **Governance and Audit:**
   The MLRO is responsible for ensuring the RBA is embedded into policy and operations. The internal audit reviews RBA implementation annually and reports findings to the Board.

Business Risk Assessment (BRA)

Turn 1 conducts a formal Business Risk Assessment (BRA) at least annually, or when material changes to the business model, technology, product offering, or regulatory landscape occur.

The BRA is led by the MLRO and reviewed by the Board. It is documented, version-controlled, and informs both the AML Policy and internal control framework.

The BRA evaluates ML/TF exposure across the following domains:

Risk Domain	**Examples of Risk Indicators**

Products Offered	P2P poker vs RNG; collusion risk; unstructured bet sizing
Payment Channels	Use of crypto, prepaid cards, unverified bank accounts
Geographic Exposure	Player base includes higher-risk countries or greylisted ones
Delivery Channels	Non-face-to-face onboarding, third party platforms
Customer Base	Prevalence of high-risk or anonymous customers
Third-Party Dependence	Reliance on vendors for KYC or game monitoring
Game Integrity	Chip dumping, bots, multi accounting, device/IP anomalies

The BRA assigns a residual risk rating (Low, Medium, High) to each domain based on:

- Inherent risk level
- Effectiveness of controls
- Historical incident data (if any)

The cumulative output of the BRA guides:

- The CRA scoring model and thresholds
- EDD triggers and internal escalation points
- Audit focus areas
- Control investments (e.g., Game Integrity tooling, KYC vendors)

The BRA is reviewed annually and updated in response to:

- New products
- Expansion into new jurisdictions
- Regulatory findings or internal incidents

See Appendix C for BRA template.

Customer Risk Assessment (CRA)

Turn 1 performs a Customer Risk Assessment (CRA) for each player upon onboarding, using a structured scoring model to determine their risk category and define the level of due diligence required.

1. Risk Rating Categories

Customers are classified as:

- **Low Risk** – standard due diligence applies
- **Medium Risk** – enhanced monitoring; review at first withdrawal
- **High Risk** – enhanced due diligence (EDD) required before withdrawal or further activity

2. Risk Factors and Scoring Matrix

Risk Factor	Low Risk (1 pt)	Medium Risk (2 pts)	High Risk (3 pts)
Jurisdiction	EU, EEA, UK, IoM	Non-FATF monitored	FATF grey/blacklisted
Payment Method	Bank card, bank transfer	E-wallets	Crypto, 3rd party transfers
Product Type	RNG Casino	Sports or Table Games	P2P Poker or Transfers
Behaviour	Normal play, consistent	Mild anomalies	Collusion, chip dumping
SOF/SOW Clarity	Payslip, bank statement	Generic income declaration	Unverifiable/unknown

PEP/Sanctions	No match	Historical PEP or close assoc	Current PEP or match flagged

Risk Level by Score:

- 1–7: Low Risk
- 8–12: Medium Risk
- 13–18: High Risk (EDD required)

3. CRA Process

A full CRA must be completed or updated:

- Before any withdrawal
- When a customer's cumulative deposits are greater than $2,000
- When any red flag or monitoring alert is triggered
- At regular intervals depending on risk rating (see Ongoing Monitoring Section)

4. Override and Documentation

- Compliance or MLRO may manually adjust a customer's risk level based on new information.
- All CRAs, scoring inputs, and override notes are stored in the customer's KYC profile.
- CRA methodology is reviewed annually or upon regulatory change.

See Appendix B.

Customer Acceptance Policy

Turn 1 applies a strict customer acceptance policy in accordance with its risk appetite and regulatory obligations. The following customer types are either not accepted or require strict conditions to proceed.

Prohibited Customers

Turn 1 will not onboard or maintain accounts for:

- Individuals residing in FATF-blacklisted jurisdictions
- Persons identified on sanctions lists (UN, EU, OFAC, UK HMT, AU)
- Third-party payment users (i.e., mismatch between account holder and payment method owner)
- Customers providing false, forged, or unverifiable documentation
- Anonymous customers (incomplete identity or address verification)

KYCAID and Game Integrity systems support the enforcement of these exclusions.

Conditional Acceptance (High-Risk Customers)

The following customer types may be accepted only under strict controls:

- PEPs or individuals linked to PEPs:
    - Subject to Enhanced Due Diligence (EDD)
    - Must be approved by the MLRO or senior management
- Crypto-funded customers:
    - Source of funds and wallet ownership must be verified
    - Behavioral monitoring is intensified

Review and Reassessment

Customer risk profiles are re-assessed:

- At the time of first withdrawal
- Upon any red flag trigger
- At regular intervals based on CRA score

Customer Due Diligence (CDD)

Turn 1 applies Customer Due Diligence (CDD) procedures in accordance with Curaçao's NOIS and AML-CFT Regulations, and FATF Recommendations 10 and 22. CDD must be completed prior to permitting withdrawals or when specific risk thresholds are met.

Customer Information Collected

At Registration (Pre-KYC):

- Full legal name
- Date of birth (18+ only)
- Residential address
- Country of residence
- Email address
- Phone number
- IP geolocation and device fingerprint

This information is used for basic customer profiling, age verification, and sanctions/PEP screening via KYCAID.

At KYC Trigger (Full CDD Required):

- Government-issued photo ID (passport, national ID, or driving licence)
- Proof of address (utility bill or bank statement dated within 6 months)
- Ownership proof of any deposit method used (card, e-wallet, crypto wallet)

Verification Method

Turn 1 uses KYCAID to perform third-party identity verification. This includes:

- Optical Character Recognition (OCR) and facial biometric matching for identity documents
- Liveness detection checks to prevent impersonation or replay attacks
- Cross-checking customer details against international sanctions and PEP watchlists
- Verification of proof of address documents (e.g., utility bill, bank statement ≤ 6 months)

- IP geolocation scoring at the time of document upload to detect jurisdictional mismatches

Email address validation occurs during registration and is used as an additional control for identity consistency and contact verification.

Customer support teams verify the successful outcome of KYCAID reports and store results securely.

Payment Method Ownership

Turn 1 requires that all deposit methods be owned by the registered customer. Verification includes:

- **Credit/Debit Cards**: Images showing first 6 + last 4 digits, name, expiry (CVV obscured)
- **E-wallets**: Screenshots showing account holder name/email and transaction history
- **Crypto Wallets**: Screenshots or video of wallet within an identifiable exchange/platform, showing ownership and deposit path

Use of third-party payment methods is prohibited and triggers escalation.

CDD Triggers

CDD must be completed or refreshed when any of the following apply:

Trigger Event	**Action Required**
First withdrawal	FULL CDD and verification
Cumulative deposits > USD $2,000	Full CDD and CRA
Within 30 days of first deposit	Full CDD is not already completed
Suspicious behaviour	CDD re-verification or EDD
High-risk CRA score	Full CDD and EDD
Use of crypto or unusual payment method	Full CDD and verification of ownership

Customers who do not complete CDD within 30 days of initial deposit are subject to account restrictions, including withdrawal holds and peer-to-peer transfer blocks.

Failure to Verify

Accounts failing verification will be:

- Placed on temporary hold (no withdrawals or transfers)
- Reviewed by Compliance for re-engagement or closure
- Flagged for STR if attempts appear fraudulent or evasive

All failed verifications are logged and retained for audit.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is applied when a customer presents a higher-than-normal risk of money laundering, terrorist financing, or regulatory exposure. EDD supplements the standard Customer Due Diligence (CDD) process and must be applied in all cases where required under Curaçao AML-CFT Regulations.

EDD Triggers

EDD is mandatory in the following situations:

- The customer is a Politically Exposed Person (PEP) or a close associate/family member
- The customer resides in or is transacting from a high-risk jurisdiction
- The customer uses **cryptocurrency** as a primary deposit method
- The customer is involved in peer-to-peer transfers exceeding $1,000 cumulatively
- A red flag has been raised during transaction monitoring or Game Integrity review
- There is uncertainty about the source of funds or wealth

EDD Measures Applied

Depending on the specific risk, one or more of the following steps are taken:

1. **Additional Document Collection**
    - Recent source of funds (SOF) proof (e.g., payslip, tax return, crypto exchange statement)

    - Source of wealth (SOW) declaration with supporting documentation (e.g., property sale, business ownership)

2. **Verification of Payment Method Ownership**
    - Credit card or wallet screenshots tied to the customer's name
3. **Senior Management Review**
    - Final EDD file must be reviewed and approved by the MLRO or Compliance Officer
    - Decision to approve, suspend, or offboard must be logged and signed
4. **Increased Monitoring**
    - High-risk accounts are flagged for transaction monitoring reviews every 30 days
    - Crypto users and P2P-active players are subject to enhanced velocity and pattern alerts

Failure to Complete EDD

If a customer fails to cooperate or the documents are inadequate:

- The account is suspended
- Withdrawals are blocked
- An STR may be filed depending on the risk profile

Documentation and Recordkeeping

All EDD cases must be fully documented, including:

- Rationale for EDD
- All documents collected and verification steps taken
- MLRO review and decision
- Any follow-up actions or STRs filed

EDD records are retained for 5 years after account closure.

Ongoing Monitoring

Turn 1 performs ongoing monitoring of all customer accounts to detect activity inconsistent with a customer's risk profile, product use, or declared source of funds. Monitoring is risk-based, using a combination of automated systems and human review.

Monitoring Tools and Data Sources

- **RunGood OÜ Platform**
  Identifies:
    - Linked accounts via IP/device/browser fingerprint
    - Multi-accounting and possible collusion
    - Rapid chip movement and unusual bet sizing
    - P2P transfer anomalies
- **Payments and KYC System**
  Flags:
    - Velocity triggers (e.g., deposit → withdrawal within 30 minutes)
    - Third-party payment methods
    - New payment instruments added post-KYC
- **KYCAID and Admin Panel Logs**
  Capture:
    - Login geolocation anomalies
    - Identity re-use across accounts
    - Failed verification attempts or document re-submissions

Trigger Events for Manual Review

An internal review is triggered when:

- A player exceeds $2,000 in total withdrawals

- A high-risk customer conducts new deposits or P2P activity
- A customer's transactional or login behavior changes significantly from their established pattern (e.g., sudden increase in deposit size, device/IP mismatch, new use of peer-to-peer transfers)

Reviews include:

- Transaction history summary
- New payment methods used
- Recent P2P or crypto activity
- Sanctions/PEP re-screening
- Document re-checks (if expired or inconsistent)

Escalation Pathways

If ongoing monitoring identifies a red flag:

- The case is escalated to the Compliance Officer or MLRO
- EDD may be initiated or updated
- STR may be filed (see PEPs and Sanctions Screening Section)
- Account access may be restricted or suspended

All alerts and investigations are documented in the compliance log and retained for 5 years.

PEPs and Sanctions Screening

Turn 1 screens customers for Politically Exposed Person (PEP) status and sanctions exposure as part of its identity verification process during KYC.

Screening Scope

Screening is performed via KYCAID and includes the following lists:

- UN Consolidated Sanctions List
- European Union Sanctions
- UK HM Treasury
- U.S. OFAC
- Australian DFAT
- Global PEP lists

Screening Timing

- Screening occurs when a customer triggers KYC (e.g. first withdrawal or cumulative deposits exceeding USD $2,000)
- Customers classified as high-risk may be re-screened as part of ongoing monitoring

Handling of Matches

- Potential matches are reviewed by the Compliance Officer
- If confirmed, the account is suspended, and the MLRO is notified
- PEPs are subject to Enhanced Due Diligence (EDD) and require senior management approval
- Sanctions matches may result in STR submission and account blocking

Peer-To-Peer Product and Transfer Risks

Turn 1 permits the use of peer-to-peer (P2P) gaming products, including poker, and allows player-to-player (P2P) transfers. These features carry elevated ML/TF risks due to the potential misuse of the platform to obscure the origin or destination of funds.

Permitted Activities

- Peer-to-peer poker formats (e.g., Texas Hold’em, Omaha)
- Player-to-player transfers within the gaming environment (subject to limits)

Risk Controls

To mitigate abuse, Turn 1 implements the following controls:

- Transfer Restrictions:
  Transfers are not permitted between accounts unless the initiating player has completed full KYC.

- Volume Limits:
  Daily and cumulative limits may apply to P2P transfers based on customer risk level or verification status.

- Monitoring for Abuse:
  Game Integrity systems monitor for:

    - Chip dumping

    - Collusive betting patterns

    - Circular transfers or laundering attempts

    - Rapid transfer–withdrawal behavior

- Escalation Procedures:
  All unusual transfer activity is flagged to the Compliance Officer and, where appropriate, escalated to the MLRO for review and possible STR filing.

- Temporary Holds:
  Turn 1 may suspend accounts or withhold funds during investigation of suspicious transfer activity.

Account Reviews

- P2P activity is reviewed during customer risk assessments and periodic monitoring cycles.

- Transfer data is retained for at least 5 years.

Transaction Monitoring and Behavioral Triggers

Turn 1 maintains ongoing monitoring of customer transactions to detect activity inconsistent with the stated or expected use of the platform. Monitoring supports the early identification of potential money laundering or fraud and is aligned with FATF Recommendations 10 and 20 and Curaçao AML-CFT Regulations.

Monitoring Scope

Transactions are monitored for unusual or suspicious patterns including but not limited to:

- Deposits from multiple unrelated sources or payment methods
- Large deposits followed by no or minimal gameplay
- Withdrawals initiated without meaningful platform activity
- Use of multiple accounts from the same IP/device
- Login attempts from high-risk jurisdictions or IP mismatch
- Rapid deposit–transfer–withdrawal activity within short timeframes
- Use of high-risk payment methods (e.g., anonymous crypto wallets)

Monitoring applies across deposits, withdrawals, in-game activity, and player transfers.

Detection and Tools

Turn 1 uses:

- Game Integrity systems to flag chip movement and gameplay behavior
- Payment and admin tools to review funding and withdrawal patterns
- Manual review by Compliance where risk is unclear or automated triggers occur

Alerts are logged for review and may result in temporary account restrictions pending further investigation.

Escalation and Action

If transactional or behavioral anomalies are identified:

- The case is reviewed by the Compliance Officer
- If the behavior is considered high-risk or unexplained, it is escalated to the MLRO
- Enhanced Due Diligence (EDD) may be initiated
- A Suspicious Transaction Report (STR) may be filed with the FIU Curaçao

All escalations and decisions are documented in the internal compliance system and retained for 5 years.

Suspicious Transaction Reporting (STR)

Turn 1 has a defined process for identifying, escalating, and reporting suspicious transactions, in line with Curaçao's National Ordinance on Reporting of Unusual Transactions (NORUT) and GCB AML-CFT Regulations.

Internal Reporting of Red Flags

- All employees and contractors must report any suspicious activity immediately to the MLRO or Compliance Officer.
- Suspicious activity may include:
    - Use of third-party or anonymous payment methods
    - Attempts to avoid or delay KYC
    - Unusual gameplay or transfer behavior
    - Large, unexplained transactions
    - Inconsistent or false documentation
- The RunGood OÜ Game Integrity team provides a daily summary of flagged accounts to the Compliance team for review.

STR Filing Process

- The MLRO reviews all red flags and determines whether they meet the threshold for reporting.
- If so, an STR is filed with the FIU Curaçao within 2 business days of the suspicion being formed.
- No customer notification is permitted. This includes:
    - Avoiding any indication to the customer that they are under review

    - Not disclosing the existence or filing of an STR

Documentation and Record-Keeping

- A copy of each STR and its supporting evidence is retained in the internal STR register.
- Records include:
    - Reason for suspicion
    - Timeline of review
    - Decision maker(s)
    - Documentation gathered
- All STR-related records are retained securely for 5 years from the date of filing.

Internal STR Form

See Appendix E for the internal STR escalation form, which must be used for all reports made to the MLRO or Compliance Officer.

Record-Keeping and Data Protection

Turn 1 retains all AML-related records in accordance with the National Ordinance on the Identification of Clients (NOIS) and the Curaçao AML-CFT Regulations (2025). Records are maintained for a minimum of five (5) years from the date:

- The business relationship is terminated; or
- The last transaction is completed — whichever is later.

Records Retained

The following records are maintained in secure, access-controlled systems:

- Customer Identification Documents:
    - ID documents (passport, national ID, driver's licence)
    - Proof of address

    - Payment method ownership verification
- Risk Assessment Records:
    - CRA scores and justifications
    - BRA documents and board approvals
- Transaction Records:
    - Deposits, withdrawals, transfers, and gameplay logs
    - Monitoring alerts and escalation notes
- Suspicious Transaction Reports (STRs):
    - Internal red flag reports
    - STRs submitted to the FIU Curaçao
    - MLRO review notes and correspondence
- Training Logs:
    - Dates, participants, materials, and assessments for AML training
- Correspondence with Regulators:
    - Communications with the FIU or Gaming Control Board

Security and Access

- All records are stored digitally in encrypted systems with restricted access
- Only authorized compliance and executive personnel may access STR records
- Records are made available upon request to the GCB or FIU Curaçao

Staff Training and Awareness

Turn 1 ensures that all relevant personnel receive AML/CTF training appropriate to their roles, in accordance with Curaçao AML-CFT Regulations (2025) and FATF Recommendation 18.

Who Must Be Trained

AML training is mandatory for all:

- Customer support agents
- Payment and KYC operations staff
- Game Integrity team members (external or internal)
- Compliance, audit, and risk personnel
- Managers involved in onboarding or account reviews

Training Content and Format

Training must cover:

- Money laundering and terrorist financing risks in gaming
- Curaçao AML-CFT legal obligations
- Customer due diligence (CDD/EDD)
- Transaction monitoring and red flags
- Suspicious transaction reporting (STR) procedures
- Tipping-off risks and confidentiality
- Role-specific escalation paths and tools (e.g., KYCAID, internal STR form)

Training may be delivered:

- Internally (by Compliance Officer or MLRO), or
- By an approved external provider

Timing and Frequency

- All new staff must complete training within 30 days of onboarding
- Refresher training is conducted at least annually

- Ad-hoc training may be provided in response to:
    - Internal audit findings
    - Regulatory updates
    - Significant changes in risk profile or product offering

Records and Documentation

- Attendance records
- Training materials
- Completion dates and test results (if applicable)

All training records are retained for five (5) years and are subject to internal audit and regulatory review.

See Appendix F for the Staff Training and Vetting Checklist.

Employee Screening and Vetting

Turn 1 screens employees, contractors, and relevant third-party personnel to ensure the integrity of individuals involved in AML-sensitive roles. This process supports the prevention of internal fraud, conflicts of interest, and reputational risk in line with Curaçao AML-CFT Regulations (2025) and FATF Recommendation 18.

Scope of Screening

Screening is mandatory for:

- Employees and contractors involved in customer onboarding, KYC, payments, withdrawals, or compliance functions
- The MLRO, Compliance Officer, and directors
- External Game Integrity partners or vendors who handle player data or behavioral review

Screening Measures

Where legally permitted and appropriate to the role, Turn 1 conducts:

- Verification of identity and legal work status
- Employment and reference checks for relevant roles
- Sanctions and PEP screening
- Criminal background checks (subject to local employment laws)
- Signed integrity declarations confirming:
    - No prior convictions for fraud, ML/TF, or financial crime
    - No known conflicts of interest related to suppliers or customers

Timing and Documentation

- Screening is conducted prior to employment or contract initiation
- Screening records (e.g. checks, declarations) are retained for 5 years after the end of employment
- Any issues flagged are reviewed by the Compliance Officer and, where necessary, escalated to the MLRO or senior management

Re-Screening

- Employees in high-risk roles may be subject to periodic re-screening (e.g. annually or if promoted to ML-sensitive positions)
- Sanctions list screening may be repeated following a regulatory update or internal red flag

Internal Audit and Policy Enforcement

Turn 1 maintains an AML/CTF internal audit process to ensure ongoing compliance with regulatory obligations, assess the effectiveness of internal controls, and identify any operational deficiencies.

Audit Function and Frequency

- An independent audit of the AML/CTF framework is conducted annually

- The audit may be performed by:
    - An internal team not involved in daily AML operations, or
    - A qualified external auditor

Audit Scope

The AML/CTF audit covers:

- Compliance with CDD, EDD, CRA, and STR obligations
- Monitoring systems and alert review processes
- Effectiveness of training programs and awareness
- Record-keeping practices and data protection
- Policy adherence by key staff and vendors
- Governance and the role of the MLRO and Compliance Officer

Reporting and Remediation

- Findings are documented in an internal audit report, reviewed by the MLRO and Board of Directors
- Corrective actions must be documented and implemented with target deadlines
- Major deficiencies are escalated to the Board for oversight

Enforcement and Disciplinary Measures

- Any breach of this Policy — including failure to report red flags, bypassing controls, or aiding customer circumvention — may result in disciplinary action up to and including termination
- All breaches must be logged and reviewed by the MLRO or Compliance Officer

---

Third-Party Providers and Outsourcing Controls

Turn 1 uses third-party vendors to support critical business functions that intersect with AML/CTF risk areas. These vendors are subject to risk-based due diligence, contractual controls, and periodic performance review in accordance with Curaçao AML-CFT Regulations (2025) and FATF Recommendations 15 and 17.

AML-Sensitive Vendors

The following providers play a direct role in Turn 1's AML/CTF framework:

- KYCAID – Identity verification, document validation, PEP and sanctions screening
- RunGood OÜ – Behavioral monitoring, linked account detection, transaction pattern alerts

Additional infrastructure vendors that support transaction traceability, player behavior oversight, and platform risk detection include:

- Praxis – Cashier system and deposit/withdrawal reporting
- RYOPS – Player account management system and poker platform
- Hub88 – Casino gaming provider with visibility on gameplay logs

Vendor Risk Review

Before onboarding, Turn 1 assesses vendors based on:

- Relevance to AML/CTF controls
- Data security and privacy practices
- Contractual protections and breach procedures
- Technical integration and audit access

Reviews are conducted by the Compliance Officer and logged internally.

Contractual Controls

Vendor contracts must include:

- Confidentiality and data protection clauses
- Breach notification and cooperation with investigations
- Service level expectations (where applicable)
- Right to terminate for compliance failures

Ongoing Oversight

- AML-sensitive vendors are reviewed at least annually
- Material failures or AML concerns are escalated to the MLRO
- Vendor records and due diligence files are retained for five (5) years after contract termination

International Sanctions

Turn 1 complies with international financial sanctions regimes and prohibits business relationships with sanctioned individuals, entities, or jurisdictions, in accordance with Curaçao AML-CFT Regulations (2025) and FATF Recommendations 6 and 7.

Prohibited Persons and Jurisdictions

Turn 1 does not permit registration, deposit, withdrawal, or play by any person who:

- Is a resident or citizen of a sanctioned jurisdiction
- Is listed on any of the following consolidated sanctions lists:
    - United Nations (UN) Consolidated List
    - European Union (EU) Sanctions List
    - UK HM Treasury Sanctions List
    - U.S. OFAC Sanctions Lists (SDN, non-SDN)
    - Australian DFAT Consolidated List
- Attempts to use payment methods or banks located in sanctioned countries

Screening and Monitoring

- All customers who reach KYC triggers are screened for sanctions exposure via KYCAID
- Matches are escalated to the Compliance Officer and reviewed by the MLRO
- If a true match is confirmed, the customer account is suspended and funds may be frozen
- A Suspicious Transaction Report (STR) is filed with the FIU Curaçao

Controls on Payments

- Transactions involving payment processors, card issuers, or crypto platforms linked to sanctioned jurisdictions are blocked
- IP addresses and BIN country codes are monitored to detect possible evasion attempts

Recordkeeping

- All sanctions screening logs, match reviews, and escalations are retained for five (5) years
- See Appendix D for the current list of prohibited jurisdictions and financial institutions

Offences, Breaches, and Disciplinary Measures

All Turn 1 employees and third-party service providers are required to comply with this AML/CTF Policy and applicable legislation. Any breach may result in internal disciplinary action and/or regulatory escalation.

Types of Breaches

Breach of AML obligations may include:

- Failing to report suspicious activity or red flags
- Allowing transactions without completed CDD/EDD
- Ignoring transfer limits or KYCAID alerts
- Mishandling customer data or STRs

- Knowingly permitting use of third-party payment methods
- Engaging in or facilitating fraud or collusion

Disciplinary Actions

Depending on severity and intent, disciplinary measures may include:

- Targeted re-training or enhanced supervision
- Formal warning or probation
- Suspension from duties
- Termination of employment or contract

The Compliance Officer or MLRO investigates all breaches in collaboration with senior management. Findings are documented and reviewed.

Regulatory Reporting

If a breach suggests criminal activity, regulatory non-compliance, or material risk exposure:

- The MLRO may escalate the matter to the Curaçao Gaming Control Board or FIU Curaçao
- Law enforcement or financial crime agencies may also be notified as appropriate

Record Retention

All breach investigations and outcomes are retained for five (5) years and are available to auditors and regulators upon request.

Policy Review and Communication

This AML/CTF Policy is reviewed at least annually and updated as required to reflect changes in regulation, business activities, or internal controls.

Triggers for Review

Policy updates may be initiated by:

- Changes to Curaçao AML-CFT legislation or FATF guidance
- Internal audit findings or compliance incidents
- Launch of new products, markets, or delivery channels
- Changes in risk profile, vendors, or payment methods

Review and Approval Process

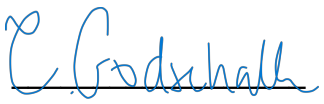
- The MLRO is responsible for leading the policy review process
- The Board of Directors must formally approve all changes
- A version-controlled log is maintained (see front page of policy)

Communication of Changes

- The latest approved version is circulated to:
    - All relevant internal teams (e.g., Compliance, Payments, Support)
    - Key third-party providers (e.g., KYCAID, RunGood OÜ)
- Staff are notified of any material policy changes and, where relevant, receive updated training

Approval and Sign-Off

This AML/CTF Policy has been reviewed and approved by the Director of Turn 1 BV.

Name	Title	Signature	Date
IGA Trust BV			
Claire Godschalk	Director		Sept 1st, 2025

Appendices

Appendix A – Definitions of Key Terms

- AML: Anti-Money Laundering – laws, regulations, and procedures to prevent criminals from disguising illegally obtained funds.
- CTF: Counter-Terrorism Financing – measures aimed at preventing and detecting the financing of terrorism.
- MLRO: Money Laundering Reporting Officer – senior person responsible for oversight of AML/CTF policies and STR filings.
- EDD: Enhanced Due Diligence – additional verification steps for high-risk customers.
- CDD: Customer Due Diligence – the process of verifying a customer's identity and assessing risk.
- PEP: Politically Exposed Person – someone who holds or has held a prominent public position, or is related to one.
- STR: Suspicious Transaction Report – a mandatory report submitted to the FIU when suspicious activity is detected.
- SOF: Source of Funds – where the money used for a transaction originates from.
- SOW: Source of Wealth – the origin of the individual's total wealth.
- CRA: Customer Risk Assessment – risk scoring framework applied to players based on defined factors.
- BRA: Business Risk Assessment – evaluation of the firm's overall exposure to ML/TF risks.
- FIU: Financial Intelligence Unit – the national agency for receiving and analyzing STRs.

Appendix B – CRA Risk Matrix

Risk Factor	Low Risk (1 pt)	Medium Risk (2 pts)	High Risk (3 pts)

Jurisdiction	EU, EEA, UK, IoM	Non-FATF monitored	FATF grey/blacklisted
Payment Method	Bank card, bank transfer	E-wallets	Crypto, 3rd party transfers
Product Type	RNG Casino	Sports or Table Games	P2P Poker or Transfers
Behaviour	Normal play, consistent	Mild anomalies	Collusion, chip dumping
SOF/SOW Clarity	Payslip, bank statement	Generic income declaration	Unverifiable/unknown
PEP/Sanctions	No match	Historical PEP or close assoc	Current PEP or match flagged

Total Score Ranges:

- 1–7: Low Risk
- 8–12: Medium Risk
- 13–18: High Risk

EDD applies to all High Risk players. CRA reviewed annually or upon major behavioral change.

Appendix C – BRA Summary Template

Business Type: Online Gaming – Peer-to-Peer Poker & Casino
Delivery Channels: Online only
Customer Base: B2C; adults aged 18 and over
Geographic Reach: Players from permitted jurisdictions excluding FATF blacklisted or sanctioned countries

Products: RNG games, Texas Hold'em, Omaha, SNGs, casino
Payment Methods: Visa, Mastercard, bank transfer, crypto
Third Parties: KYCAID (KYC), RunGood OÜ (game integrity monitoring)

Inherent Risks:

- High-risk jurisdictions
- Crypto payments
- Peer-to-peer transfer misuse
- Synthetic identity fraud

Controls in Place:

- Daily sanctions re-screening (KYCAID)
- CRA scoring and EDD triggers
- Behavioral monitoring (RunGood OÜ)
- Withdrawal thresholds
- STR escalation protocols

Residual Risk Rating: Medium
Review Date: [Insert date annually]
Approved by: [MLRO and Board]

Appendix D – Sanctioned Jurisdictions List

Players from the following countries may not be onboarded, and existing customers will be offboarded if verified to reside here:

- Afghanistan
- Belarus
- Cuba
- Iran

- North Korea
- Russia (including occupied Ukrainian territories)
- Syria
- Sudan
- South Sudan
- Myanmar (Burma)
- Venezuela (PEPs and public officials only)
- FATF-designated jurisdictions under increased monitoring

Sources: United Nations, EU, UK HMT, OFAC, FATF

This list is reviewed quarterly or upon official updates.

Appendix E – Internal Suspicious Transaction Report (STR) Form

INTERNAL STR FORM (Confidential)

- Date of Report: _____
- Reported By: _____
- Department: _____
- Customer Username/ID: _____
- Transaction Details / Summary: _____
- Reason for Suspicion:
  - ☐ Large withdrawal with minimal play
  - ☐ Use of third-party payment
  - ☐ Sanctions/PEP match
  - ☐ Unusual login/IP/device activity
  - ☐ Refusal to complete EDD
  - ☐ Other: _____

Narrative (Chronological Summary):

Actions Taken:
☐ Account restricted in line with standard withdrawal/KYC policy
☐ Withdrawal blocked
☐ Documents requested
☐ Alert sent to MLRO
☐ STR filed to FIU Curaçao (Date: _____)

MLRO Decision:
☐ STR submitted to FIU
☐ Enhanced monitoring only
☐ No further action

Appendix F – Training and Vetting Checklist

Employee Name: _____
Position: _____
Date Joined: _____
Supervisor: _____

Pre-Employment Vetting:

☐ Identity verified
☐ Work history confirmed
☐ Sanctions and PEP screening
☐ Criminal background check (where legal)
☐ Signed integrity declaration

Initial AML Training Modules:

☐ AML/CTF Overview
☐ Customer Risk and CDD
☐ EDD and SOF/SOW Handling
☐ STR Identification and Escalation
☐ Role-Specific Risks

Annual Training Tracker:

Date	Format	Content	Completed	Verified By

All staff must complete AML training at least annually and upon any role change.

End of Full AML/CTF Policy Document – Version 1.1