

Anti-Money Laundering & Counter-Terrorist Financing Policy

Seven Days B.V.

Applicable to: Weeekly | Weeekly Rivals | Casino

Prepared in alignment with:

National Ordinance on Identification of Clients when Rendering Services (NOIS)

National Ordinance on the Reporting of Unusual Transactions (NORUT)

Sanctions National Ordinance & Kingdom Sanction Act

GCB Regulations for Combating ML/FT/FP, January 2025

Version 1.0

Effective Date: [ON LICENCE GRANT]

Issued by: Seven Days B.V.

Curacao Gaming Authority Licence No. [LICENCE NUMBER]

Policy Title	AML/CTF Policy
Entity	Seven Days B.V.
Platforms	Weeekly, Weeekly Rivals, Casino
Approving Official	Senior Management / Board of Directors
Responsible Office	Compliance Officer
Effective Date	Effective on Curaçao Gaming Authority licence grant
Next Review Date	Twelve months after effective date, or earlier upon material change
Version	1.0
Contact	compliance@weeekly.com

1. Policy Statement

Seven Days B.V. (“the Company”) operates three distinct gaming products under the domain *www.weeekly.com*: **Weeekly** (a weekly raffle and competition platform), **Weeekly Rivals** (a competitive wagering leaderboard), and **Casino** (a standard casino product). The Company is incorporated under the laws of Curaçao; this policy and its associated frameworks shall come into full effect immediately upon the granting of the Curaçao Gaming Authority (CGA) license.

The Company is firmly committed to preventing its platforms from being used for money laundering (ML), terrorist financing (TF), or the financing of proliferation of weapons of mass destruction (FP). This policy establishes the Company’s AML/CTF/CFP framework in compliance with:

- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99);
- The Sanctions National Ordinance (N.G. 2014, no. 55);
- The Kingdom Sanction Act (N.G. 2016, no. 54);
- The GCB Regulations for Combating ML/FT/FP (January 2025, effective April 10, 2025);
- FATF Recommendations and CFATF standards.

This policy applies to all employees, contractors, third-party service providers, and agents acting on behalf of the Company across all three platforms. Compliance with this policy is mandatory and non-negotiable.

2. Purpose

The purpose of this policy is to:

- Establish a risk-based framework to identify, assess, and mitigate the risk of ML/TF/FP across the Company’s platforms;
- Define the Customer Due Diligence (CDD) procedures, thresholds, and escalation processes applicable to Weeekly, Weeekly Rivals, and Casino;

- Set out the Company's obligations for detecting and reporting unusual transactions to the Curaçao Financial Intelligence Unit (FIU);
- Ensure the Company maintains records in compliance with the five-year retention requirement under Curaçao law;
- Provide the Compliance Officer, staff, and relevant third parties with clear guidance on their responsibilities;
- Demonstrate compliance readiness to the Curaçao Gaming Authority (CGA) and the Gaming Control Board (GCB) during examination.

3. Audience

This policy applies to all individuals and entities associated with Seven Days B.V., including:

- All employees and senior management;
- The appointed Compliance Officer;
- Contractors and temporary staff involved in onboarding, payments, or compliance functions;
- Third-party KYC/AML vendors and technology providers;
- Payment processing partners and blockchain forensic providers;
- Any agent or group company acting on behalf of the Company.

Platform-specific applicability: Where this policy refers to thresholds, triggers, or product mechanics, provisions apply to the relevant platform(s) as indicated. Weeekly Rivals operates as a competitive wagering product on a leaderboard with a fixed equal starting balance for all entrants; Weeekly operates as a raffle platform; Casino operates as a standard online casino. All three share the same legal entity and this unified AML/CTF framework.

4. Definitions

Term	Definition
AML/CTF	Anti-Money Laundering and Counter-Terrorist Financing.
BRA	Business Risk Assessment: an annual documented assessment of ML/TF/FP risks facing the Company.
CDD	Customer Due Diligence: the set of identification, verification, and monitoring measures applied to players.
CRA	Customer Risk Assessment: a player-specific risk profile derived from the BRA categories.
CAP	Customer Acceptance Policy: the policy that sets CDD levels based on CRA outcomes.
EDD	Enhanced Due Diligence: heightened CDD measures applied to high-risk players or transactions. EDD layers on top of Level 2 verification (see Section 5.4) and is determined by the player's risk rating, not by transaction volume alone.
FIU	Financial Intelligence Unit Curaçao, the authority to which Unusual Transaction Reports are filed.

Term	Definition
Financial Transaction	Deposits and withdrawals on the platform. Gambling transactions (wagers and winnings in Weeekly Coins) are explicitly excluded from the definition of financial transactions under Curaçao law.
FP	Financing of Proliferation of weapons of mass destruction.
FT / TF	Financing of Terrorism.
GCB	Gaming Control Board of Curaçao.
CGA	Curaçao Gaming Authority.
Level 1 / Level 2	The two procedural KYC tiers applied by the Company. Level 1 is the standard onboarding identity check applied to every player. Level 2 is the enhanced verification check (government photo ID plus biometric/liveness) triggered by the threshold, suspicion, prize, or first-withdrawal triggers set out in Section 5.4.
ML	Money Laundering.
ML Stages	The three conceptual stages of money laundering recognised by FATF and applied in this policy: (i) Placement - introducing illicit proceeds into the financial system; (ii) Layering - separating proceeds from their criminal origin through complex or successive transactions; (iii) Integration - reintroducing the laundered funds into the legitimate economy in a form that appears licit. The Company's Transaction Monitoring controls are designed to detect indicators across all three stages.
NAf.	Netherlands Antillean Florin: The local currency unit utilized in regulatory thresholds. For compliance reporting and historical regulatory continuity (such as under the Gaming Control Board (GCB) AML/CFT Regulations), it corresponds to the prior ISO 4217 code ANG, which has been legally succeeded by the current ISO 4217 code XCG (Caribbean Guilder) at a 1:1 parity.
PEP	Politically Exposed Person: an individual who holds or has held a prominent public function.
SDD	Simplified Due Diligence: reduced CDD measures permitted in verified low-risk situations.
STR / UTR	Suspicious Transaction Report / Unusual Transaction Report: a report filed with the FIU.
Key Person	A natural person who, either by name or de facto, has indirect or direct control of, or significant influence on, a licensee's management or assets, or the approval or implementation of a licensee's operational policy. Key Persons are prohibited from playing Games of Chance on the platform.
UBO	Ultimate Beneficial Owner: the natural person(s) who ultimately own or control the customer.
USDT / USDC	Tether (USDT) and USD Coin (USDC): the only accepted stablecoins on the platform.
Vulnerable Person	A person under 18 years of age; a person who has no or insufficient control over their gambling behavior and is, or threatens to become, addicted to Games of Chance; a person who has been banned from playing any Game of Chance either by force or at

Term	Definition
	their own request; or a person who has been declared bankrupt, or has otherwise lost the control or disposal of all or part of their property.
Weeekly Coins	A non-withdrawable virtual in-platform currency used for wagering. Coin transactions are gambling transactions, not financial transactions.

5. Policy Implementation

5.1 Business Risk Assessment (BRA)

The Company conducts a documented Business Risk Assessment at least annually and upon any material change to its operating environment. The BRA is approved by the Board of Directors and made available to the GCB/CGA upon request.

The BRA evaluates risks across the following four dimensions, applied consistently across Weeekly, Weeekly Rivals, and Casino:

Customer Risk

Risk arising from the nature and profile of users. Higher-risk customer categories include:

- Players with multiple or irregular income sources;
- Politically Exposed Persons (PEPs) and their family members or close associates;
- High-volume depositors inconsistent with known income profile;
- Players exhibiting structuring behavior (deliberately splitting transactions);
- Players using third-party wallets or accounts;
- Players from high-risk jurisdictions.

Geographical Risk

Risk arising from the player's country of residence, nationality, or the origin of funds. The Company maintains an internal country risk list informed by:

- FATF list of High-Risk Jurisdictions subject to a Call for Action;
- FATF list of Jurisdictions under Increased Monitoring;
- CFATF Public Statement;
- OFAC Sanctions List;
- Transparency International Corruption Perceptions Index;
- U.S. Department of State INCSR Jurisdictions of Concern.

Product, Service and Transaction Risk

All three platforms are crypto-based and accept only USDT and USDC, which reduces certain anonymity risks compared to cash or privacy coin environments. However, the following product-level risks are acknowledged:

- Deposit and withdraw with minimal play patterns (account use as a pass-through);
- Structuring deposits across multiple sessions to avoid thresholds;
- Funds originating from mixing services, tumblers, or high-risk wallet sources;

- Use of Weeekly Coins to create the appearance of gaming activity without genuine wagering intent;
- Rivals leaderboard manipulation or collusion to engineer prize outcomes;
- Multiple accounts held by a single beneficial owner.
- In-house game integrity risks within Casino, including game-logic exploitation, RTP manipulation, and bonus-abuse patterns specific to proprietary game titles.
- RNG integrity for in-house games, including reliance on RNG certification, seed-handling controls, and operational change management for game logic.

The Company explicitly prohibits the use of privacy coins, mixing services, and exchange hot wallets for deposits or withdrawals.

Distribution Channel Risk

All three platforms operate exclusively online and on a non-face-to-face basis. This increases the inherent risk of identity fraud and impersonation. The Company manages this risk through a tiered approach:

- Automated Sanctions & PEP Screening: Immediate screening of all users against international sanctions and Politically Exposed Persons (PEP) lists upon registration.
- Technical Perimeter Controls: Use of IP geolocation, VPN/proxy detection, and device fingerprinting to identify high-risk jurisdictions or obscured identities at the point of entry.
- Blockchain Forensic Monitoring: Continuous wallet screening via a recognised blockchain analytics provider to detect links to illicit activity or high-risk sources of funds.
- Trigger-Based Document Verification: Mandatory document-based KYC, including biometric and liveness checks, via a regulated third-party provider once specific activity thresholds or risk triggers are met (as detailed in Section 5.4).

Technological Development Risk Assessment

Prior to launching any new product feature, payment method, game type, or delivery mechanism, the Company conducts a documented technology risk assessment to identify and mitigate any new ML/TF/FP vulnerabilities introduced.

5.2 Customer Risk Assessment (CRA)

A Customer Risk Assessment is conducted for each player at or before the point of establishing a business relationship (i.e., account opening). The CRA assigns each player an initial risk rating of Low, Medium, or High based on the risk categories established in the BRA. The CRA is revised when:

- Level 2 verification is initiated;
- Transaction patterns deviate materially from the established profile;
- New information is obtained (e.g., PEP status identified during ongoing screening);
- A player changes their payment instrument, deposit pattern, or jurisdiction.

The CRA outcome determines the level of CDD applied, as set out in the Customer Acceptance Policy.

5.3 Customer Acceptance Policy (CAP)

The CAP defines which players the Company will onboard, at what CDD level, and the circumstances under which a business relationship is declined or terminated.

CDD Tiers

Risk Level	CDD Tier	Measures Required	Monitoring
Low	Simplified CDD (SDD)	Level 1 onboarding (name, address, DOB, PEP & sanctions screening); Level 2 verification triggered upon reaching Naf. 4,000 threshold (or earlier on suspicion, prize-win, or first-withdrawal trigger - see Section 5.4)	Standard periodic review
Medium	Standard CDD	Level 2 verification, full CRA, source of funds declaration	Ongoing transaction monitoring
High	Enhanced CDD (EDD)	Level 2 verification plus EDD: independent source of funds/wealth documentation; senior management approval required	Enhanced monitoring; periodic EDD refresh
PEP	Enhanced CDD (EDD)	Level 2 verification plus all EDD measures, senior management approval, source of wealth verification, and enhanced ongoing monitoring	Enhanced monitoring; periodic EDD refresh
Denied	N/A — Relationship Declined	Sanctioned individuals; falsified documents; prohibited jurisdictions; KYC refusal beyond 30-day window	N/A

Declined Players

The Company will decline or terminate a business relationship where a player:

- Appears on UN, EU, or local Curaçao sanctions lists;
- Is located in or originates funds from a prohibited jurisdiction;
- Submits falsified, expired, or unverifiable identity documents;
- Refuses or fails to provide required KYC information within a 30-day window;
- Uses privacy-enhancing tools to obscure fund origins;
- Exhibits behavior consistent with ban evasion, account sharing, or multi-account abuse;
- Qualifies as a Key Person of the Company (i.e., any director, senior officer, or person with direct or indirect control over the Company's management or assets) - such persons are prohibited from playing Games of Chance on the platform;
- Is a Vulnerable Person as defined under LOK Art. 1.1(h): a minor (under 18), a person with insufficient control over their gambling behavior, a person who has been banned from games of chance, or a person who has been declared bankrupt or has otherwise lost control of their property.

Credit Prohibition: The Company is strictly prohibited from providing players with any form of credit, or from acting as an intermediary in providing such credit. This prohibition is absolute and applies across all three platforms.

5.4 Customer Due Diligence (CDD)

The Company applies a two-tier KYC model to give effect to the CDD measures required under the GCB AML/CFT Regulations and the Customer Acceptance Policy at Section 5.3. The two tiers are procedural - they describe when identity verification is required and at what depth. They sit alongside (and do not replace) the substantive risk-rating and EDD framework set out in the CDD Tiers table at Section 5.3, which determines how much diligence is required based on the player's risk profile. A player will always be at one Level (1 or 2) and at one Risk Rating (Low / Medium / High / PEP); EDD applies to High-risk and PEP players regardless of Level.

Level 1: Standard Onboarding - Minimum Onboarding Requirements (all players, all platforms)

At account creation, regardless of deposit level, the Company collects:

- Full legal name;
- Permanent residential address;
- Date of birth;
- PEP status screening (against recognised regional and international PEP databases).
- Sanctions screening (UN, EU, and any locally published Curaçao sanctions list).

Free-to-Play Participation: Users participating exclusively in free-to-play campaigns (no purchase required) remain at **Level 1 (Low Risk)**. For these users, the minimum onboarding identifiers above (name, address, date of birth, PEP and sanctions screening) are still collected. Transition to Level 2 verification is mandatory upon meeting any of the triggers set out in Section 5.4.

Level 2: Enhanced Verification - Triggers and Requirements

Level 2 verification - comprising government-issued photo ID, biometric/liveness check, and the additional CDD elements set out below - is triggered by any one of the following four pathways. Each pathway operates independently; the first to apply governs.

(a) Threshold trigger: cumulative deposits and/or withdrawals reach NAf. 4,000 (running basis from establishment of the business relationship). Weeekly Coin wagers and winnings are gambling transactions and are explicitly excluded from this calculation. Detailed account-state consequences for this pathway are set out under "What Happens When the NAf. 4,000 Threshold Is Reached" below.

(b) Suspicion trigger: the Compliance Officer (or any staff member, escalating to the Compliance Officer) detects a suspicion of money laundering, terrorism financing, proliferation financing, fraud, or any other indicator of unusual activity, regardless of transaction value.

(c) Prize trigger: the player becomes entitled to receive any prize or other payout on Weeekly, Rivals, or Casino. No prize will be released to the player before Level 2 verification is complete.

(d) First-withdrawal trigger: the player attempts to make their first withdrawal from the platform, regardless of amount. Level 2 verification must be completed before the first withdrawal is processed. Subsequent withdrawals do not re-trigger Level 2 unless another trigger applies.

Level 2 verification comprises:

- Identification: Full name, permanent address, date of birth, place of birth, nationality, and identity number;

- Verification: Government-issued unexpired photo ID (passport, national ID, or driver's licence); proof of address (utility bill or bank statement not older than six months); biometric/liveness check via regulated third-party provider;
- Customer Risk Assessment: Confirmation or revision of the player's Low/Medium/High risk rating;
- Purpose and Nature: Confirmation of purpose of the account and expected level of activity;
- Beneficial Owner: Declaration that the player is registering and transacting on their own behalf; where a beneficial owner other than the player is identified, their identity must be verified.
- Account Type Restriction: Corporate, business-participant, syndicate, and any other non-individual accounts are not accepted on the Platform. All player accounts must be opened and operated by a natural person registering and transacting on their own behalf. Where the Compliance Officer becomes aware that a player is registering or transacting on behalf of one or more third parties, the relationship is treated under the Termination of the Business Relationship procedure in this Section 5.4 and an Unusual Transaction Report is filed where appropriate.

What Happens When the NAf. 4,000 Threshold Is Reached (Level 2 Threshold Trigger)

This sub-section describes the operational consequences of the Level 2 threshold trigger at (a) above. Equivalent account actions apply, with appropriate variation, where Level 2 is triggered by the suspicion or prize pathways.

If the threshold is reached via a deposit: the player cannot make further deposits or withdrawals until Level 2 verification is complete. The player may continue to use funds already in their account for gameplay.

If the threshold is reached via a withdrawal request: a full account freeze is applied. The player cannot continue playing until Level 2 verification is complete.

If required Level 2 documentation is not received within 30 days of the threshold being reached:

- The business relationship is terminated;
- If no suspicion of ML/TF exists, funds are returned to the same wallet or account from which they were deposited;
- If there is a reasonable suspicion of ML/TF/FP, the Compliance Officer determines whether funds are blocked and files an Unusual Transaction Report (UTR) with the FIU. The risk of tipping off the player must be considered before any account action is taken.

Enhanced Due Diligence (EDD)

EDD is a substantive layer of additional diligence that operates on top of Level 2 verification. EDD is determined by the player's risk rating (High or PEP) or by specific risk indicators - not by transaction volume alone - and applies for the duration of the relationship. A player subject to EDD must always have completed Level 2 verification.

EDD is applied where the CRA identifies a high-risk player or where specific risk indicators are present, including:

- Residency in or funds originating from a high-risk jurisdiction;
- PEP status;
- Products or transaction patterns that may favour anonymity;
- High deposit volumes inconsistent with declared income;
- Use of new technologies or payment mechanisms at launch.

EDD measures include:

- Obtaining additional identifying information (occupation, previous addresses, public database checks);
- Source of funds documentation (e.g., payslips, bank statements, investment records);
- Source of wealth documentation (e.g., business ownership, inheritance records);
- Senior management approval to establish or continue the relationship;
- Enhanced and more frequent transaction monitoring.

For PEPs specifically, senior management approval is mandatory before onboarding, and source of wealth must be independently verified. Enhanced monitoring applies for the duration of the relationship.

Termination of the Business Relationship

Where Level 2 verification or EDD obligations cannot be fulfilled, the Company will close or suspend the account and retain records of all attempts made to obtain required documentation. Where a player later provides the required documentation following account closure, the Compliance Officer reassesses the ML/TF risk before deciding whether to reinstate the relationship.

5.5 Ongoing Monitoring

Identity Monitoring

The Company maintains accurate and up-to-date identification data for all players. Identification data is refreshed:

- On key events (e.g., change of payment instrument, change of residential address);
- Upon expiry of identity documents;
- Periodically, on a risk-sensitive basis, for high-risk players.

Sanctions screening against UN and EU lists (and any locally published Curaçao list) is conducted at onboarding and on an ongoing basis throughout the customer lifecycle. Where a player is identified as being on a sanctions list, funds are frozen immediately without prior notice; a report is filed with the FIU, and the Company follows the Process for the Freezing of Resources published in the National Gazette.

Transaction Monitoring

The Company employs a combination of automated rule-based systems and manual review to monitor all financial transactions (deposits and withdrawals) for unusual activity. Monitoring systems are calibrated to detect:

- Deposits with minimal or no associated gameplay (pass-through behavior);
- Structuring: multiple transactions individually below the NAf. 4,000 CDD threshold or NAf. 5,000 UTR threshold that cumulatively meet or exceed either threshold.
- Rapid cycling of funds: deposit followed by immediate withdrawal with minimal play;
- Wallet addresses linked to mixing services, darknet markets, sanctioned entities, or high-risk sources;
- Significant deviations from a player's established wagering profile;

All automated alerts are reviewed by the Compliance team. Transactions that cannot be adequately explained are escalated for an unusual transaction report filing with the FIU.

Where transactions deviate materially from the player's established profile, the Compliance Officer may request source of funds information from the player (and, where appropriate, supporting documentation) before further activity is permitted. Failure to provide a satisfactory explanation or supporting documentation is treated as an indicator of unusual activity and may result in an Unusual Transaction Report being filed with the FIU and the relationship being managed under the Termination procedure in Section 5.4.

Anti-Mixing and Privacy-Enhancing Technology Controls

The Company prohibits the use of mixers, tumblers, coin-join services, anonymity-enhanced cryptocurrencies, and other privacy-enhancing technologies designed to obscure the origin or destination of funds. The Company accepts only USDT and USDC; no other cryptocurrency is supported. Every deposit and withdrawal is screened against blockchain analytics indicators (including known mixer addresses, darknet-market clusters, sanctioned wallet clusters, and high-risk-exchange clusters) via a recognised blockchain analytics provider. A wallet exhibiting direct or indirect exposure to mixing services or other privacy-enhancing technology will trigger a transaction block, an account review, and where appropriate an Unusual Transaction Report. Where the Company becomes aware that a player has used or attempted to use anonymity-enhancing technology in connection with the platform, the matter is escalated to the Compliance Officer for review, and the business relationship may be terminated and the funds made subject to the Termination of the Business Relationship procedure set out in Section 5.4.

Ban Evasion and Multi-Account Detection

The Company maintains controls to prevent and detect ban evasion, multi-accounting, and account sharing, including for players who are subject to self-exclusion under the Self-Exclusion Policy or who have previously been declined or terminated under Section 5.3. Detection methods include device fingerprinting, IP and connection-pattern analysis, payment-method matching, and identity-data cross-checks at onboarding. Peer-to-peer transfers between player accounts on the platform are prohibited; any attempt to circumvent this prohibition is treated as a red flag and escalated to the Compliance Officer. Where multi-accounting or ban evasion is identified, all linked accounts are suspended pending review; funds are subject to the Termination of the Business Relationship procedure, and the matter is reviewed for filing an Unusual Transaction Report.

Geo-Location and Device Integrity Monitoring

The Company applies IP-based geo-blocking to prevent access from prohibited jurisdictions and from comprehensively sanctioned jurisdictions. As a complementary control, device timezone, language, and connection-pattern signals are cross-checked against the player's declared country of residence and IP-based location at onboarding and on an ongoing basis. Material discrepancies (for example, a device timezone consistent with a prohibited jurisdiction while the IP address resolves to a permitted jurisdiction) are treated as indicators of potential VPN, proxy, or location-spoofing use and trigger an account review. Persistent or unexplained discrepancies are grounds for suspension and, where appropriate, termination of the business relationship under Section 5.4 and filing of an Unusual Transaction Report.

5.6 Reliance on Third Parties to Perform CDD

The Company may rely on regulated third-party providers - including a regulated identity verification provider and a recognised blockchain analytics provider - to perform elements of CDD. The following conditions apply:

- The Company obtains CDD information from the third party immediately upon completion;
- A written agreement is in place ensuring that copies of identification data and relevant CDD documentation will be made available to the Company on request;
- The third party is regulated, supervised, or monitored for CDD and record-keeping compliance equivalent to the standards in this policy;
- The third party operates in a jurisdiction assessed as low-to-medium country risk.

The Company retains full responsibility for CDD compliance at all times. The decision to onboard or continue a relationship with a player cannot be delegated to any third party. Customer risk assessments, PEP screening, and ongoing monitoring remain in the Company's direct responsibility regardless of third-party involvement.

5.7 Reporting of Unusual Transactions

Obligation to Report

The Company is required to detect and report unusual transactions to the FIU Curaçao without delay, via the goAML reporting portal. The Company has registered with the FIU and maintains access to the goAML system. All reports and supporting documentation are submitted in English.

Unusual Transaction Thresholds and Indicators

The following transactions are deemed unusual and must be reported:

- Any financial transaction (single or cumulative series within a gaming day) of NAf. 5,000 or more, including on-chain transfers between the Company's custodial wallets and a player's account, deposits, and withdrawals.
- Any transaction involving a person or entity named on a UN or EU sanctions list;
- Any transaction where there is a reasonable basis to suspect ML/TF/FP, regardless of amount.

Internal Reporting Process

All staff who identify a potential unusual transaction must report it immediately to the Compliance Officer using the Company's approved internal reporting format, together with all supporting documentation (KYC records, transaction logs, communications).

The Compliance Officer reviews each internal report for completeness and accuracy, determines whether an external UTR must be filed with the FIU, and documents the decision with reasons. Where a transaction is not externally reported, the reasons are recorded and signed off by the Compliance Officer.

Prohibition on Disclosure (Tipping Off)

The Company, its directors, officers, and employees are strictly prohibited from disclosing to a player or any third party that a UTR has been filed or that an investigation is underway. This prohibition applies regardless of the player's request for information. Where the Compliance Officer determines that performing CDD would tip off a player, the CDD process may be suspended and a UTR filed directly.

Where account action is required following a UTR (e.g., blocking or freezing), drastic action should be avoided unless no other course is available, as unjustified action may alert the player. Increased monitoring and additional UTR filings are the preferred responses where possible.

Record Keeping

The Company retains all records relating to CDD, transactions, monitoring alerts, UTRs, and associated communications for a minimum of five (5) years from the end of the business relationship or the date of the occasional transaction, whichever is later. Records are:

- Stored securely and in encrypted form;
- Timestamped and attributable to individual players;
- Sufficient to permit full reconstruction of individual transactions;
- Made available to the GCB, CGA, FIU, and other competent Curaçao authorities upon lawful request.

Data Centre Requirement: All digital records of specific critical information about players, their gaming transactions, and their financial transactions must be kept available to the CGA at all times on a server of a Tier-IV certified data center registered in Curaçao. The Company shall ensure its infrastructure and hosting arrangements comply with this requirement prior to the commencement of licensed operations.

Regulatory Reporting Obligations: In addition to AML/CTF reporting, the Company is required to:

- File incident reports with the CGA within 24 hours of any gaming security breach, equipment failure, fraud attempt, or event posing a serious threat to the reliable organisation of Games of Chance;
- Submit amendment reports to the CGA twice yearly, by 15 June and 15 January, covering any changes to the operations manual;
- Submit annual financial statements to the CGA by 30 June of each following calendar year.

5.8 Anti-Money Laundering Compliance Program

5.8.1 System of Internal Policies, Procedures and Controls

The Company maintains a written AML/CTF compliance program that is approved by senior management and the Board of Directors. This program includes this policy and is supplemented by detailed operational procedures covering CDD workflows, UTR escalation, sanctions screening, and staff conduct. The program is communicated to all relevant employees and reviewed whenever regulatory changes, new products, or material risk events occur. In the absence of such changes, the program is reviewed annually.

5.8.2 Compliance Officer

The Company formally designates a Compliance Officer who is a senior officer at management level and independent from gaming operations. The Compliance Officer has direct access to all CDD records, transaction data, and monitoring systems and has the authority to act independently on compliance matters.

The Compliance Officer's responsibilities include:

- Designing and implementing the AML/CTF compliance program;
- Verifying adherence to Curaçao AML/CTF laws and GCB/CGA regulations;
- Overseeing CDD processes and approving high-risk onboarding decisions;

- Reviewing all internally reported unusual transactions and determining whether external reporting to the FIU is required;
- Maintaining records of all UTRs filed internally and externally;
- Designing and maintaining the internal procedure for account blocking/freezing following UTR filing, with attention to the risk of tipping off;
- Organizing and overseeing AML/CTF training for staff;
- Remaining informed of developments in ML/TF methods and regulatory guidance;
- Providing regular compliance reporting to senior management and the Board;
- Liaising with the GCB, CGA, FIU, and other competent authorities as required.

For all compliance queries, contact: *compliance@weeekly.com*

5.8.3 Employee Screening and Training

All employees and contractors involved in customer-facing functions, payments, or compliance roles are subject to criminal background screening prior to engagement.

AML/CTF training is mandatory for all relevant personnel and is delivered:

- Upon onboarding (all new staff who handle transactions or customer accounts);
- Annually as a refresher for all relevant staff;
- Upon material regulatory change or following a significant compliance incident.

Training covers: the nature and process of ML/TF/FP; red flag indicators relevant to each platform; CDD and KYC workflows (including Level 1 and Level 2 procedures); sanctions screening procedures; the escalation and UTR reporting process; the prohibition on tipping off; and the consequences of non-compliance. Training records, including content, attendees, dates, and any assessment of results, are maintained for audit purposes.

5.8.4 Independent Audit Function

The AML/CTF compliance program is subject to independent audit at least annually, conducted by either an adequately resourced internal audit team not involved in compliance functions, or an external auditor. Auditors must hold relevant AML/CTF qualifications (e.g., CAMS, AMLFC) and a minimum of two years' experience in AML/CTF compliance.

The audit scope includes:

- Review of AML/CTF policies, procedures, and controls manuals;
- Compliance management effectiveness;
- Transaction testing, including sampling of transactions at and beyond reporting thresholds;
- Assessment of training adequacy and staff awareness;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of internal reporting and UTR filing processes;
- Adequacy of record retention systems;
- Responsiveness of the Board to previous audit findings.

Audit findings and deficiencies are reported to senior management and the Board with a request for prompt corrective action by a specified deadline.

6. Compliance and Consequences of Non-Compliance

Compliance with this policy is mandatory for all employees, contractors, and agents of Seven Days B.V. Violations of this policy or of applicable Curaçao AML/CTF legislation may result in:

- Internal disciplinary action, up to and including termination of employment or contract;
- Civil and criminal liability under the NOIS, NORUT, Sanctions National Ordinance, and the Kingdom Sanction Act;
- Administrative sanctions imposed by the GCB or CGA, including suspension or revocation of the gaming licence - in particular, failure to comply with AML/CTF obligations is a mandatory revocation ground;
- Referral to and investigation by the FIU, Curaçao Police, or other competent authorities;
- Reputational damage to the Company and its platforms.

goAML Registration: Registration with the FIU's goAML reporting portal is a mandatory condition of the Gaming Licence. The Company must be registered with goAML prior to licence issuance and must maintain this registration at all times. Failure to maintain goAML registration is a ground for licence denial or revocation.

Employees who become aware of actual or suspected non-compliance are required to report this immediately to the Compliance Officer at compliance@weeekly.com. The Company will not penalise any employee who reports a concern in good faith.

7. Related Information

This policy should be read in conjunction with the following documents and legislative requirements:

- GCB Regulations for Combating ML/FT/FP (January 2025);
- National Ordinance on Games of Chance (LOK), December 2024 (Year 2024, No. 157) — in particular: Art. 1.1 (definitions including Vulnerable Person and Key Person); Art. 1.3(b) (Key Person gaming prohibition); Art. 1.4(c) (credit prohibition); Art. 2.2(2)(k) (goAML registration as licence condition); Art. 5.4(2) (12-month irrevocable self-exclusion minimum); Art. 5.5 (Curaçao law/courts jurisdiction clause mandatory in T&Cs); Art. 5.9(1)(j) (Tier-IV data centre requirement); Art. 5.10(4)(6) (incident and amendment reporting timelines); Art. 5.11(3) (annual financial statements by 30 June);
- NOIS (N.G. 2017, no. 92);
- NORUT (N.G. 2017, no. 99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- FATF 40 Recommendations;
- Seven Days B.V. KYC Policy;
- Seven Days B.V. Deposit & Withdrawal Policy;
- Seven Days B.V. Privacy Policy;
- Seven Days B.V. Responsible Gambling & Self-Exclusion Policy;
- Seven Days B.V. Terms & Conditions;
- Seven Days B.V. Free-to-Play / Promotional Phase Terms;
- Ministerial Decree - Indicators for Unusual Transactions (N.G. 2015, no. 73).

8. Contact Information

For all questions, reports, or concerns regarding this policy:

Compliance Officer	[To Be Appointed prior to licence grant]
Email	compliance@weeekly.com
Platform Support	support@weeekly.com
Website	www.weeekly.com
Regulator	Curaçao Gaming Authority (CGA) / Gaming Control Board (GCB)
FIU (Unusual Transactions)	FIU Curaçao - via goAML portal

9. Policy History

Version	Effective Date	Author	Summary of Changes
1.0	May 2026 (drafted; effective on licence grant)	Seven Days B.V.	Initial policy.

10. Policy URL

This policy is published internally and made available to the GCB/CGA upon request. Where published on the Company website, it will be accessible at: <https://weeekly.com/aml>