

Anti-Money Laundering and Counter-Terrorist Financing Policy

Trendy Games B.V (2025)

Introduction & Purpose

Trendy Games B.V. (operating the **FridayBet.com** platform) is committed to full compliance with Curaçao's Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) laws and international standards. This policy outlines the company's AML/CFT program, aligning with our Business Risk Assessment (BRA) and Curaçao's legal framework, including the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Regulation Indicators of Unusual Transactions (Regeling Indicatoren Ongebruikelijke Transacties, 2015 as amended in 2024), the 2025 AML/CFT Regulations for gaming operators, and the National Ordinance on Games of Chance (LOK). It also incorporates relevant FATF 40 Recommendations and CFATF guidance as applicable to Curaçao. The purpose of this policy is to prevent Trendy Games' platform from being used for money laundering (ML), terrorist financing (TF), or other illicit financial activity, by clearly setting out our risk-based controls, due diligence procedures, monitoring and reporting obligations, and staff responsibilities. All directors, officers, employees, and relevant contractors of Trendy Games B.V. must adhere to this policy. Senior management endorses this policy, which is subject to periodic review (at least annually or upon significant changes) to ensure ongoing effectiveness and compliance with evolving regulations.

Risk-Based Approach & Business Risk Assessment

Trendy Games B.V. utilizes a Risk-Based Approach (RBA) to AML/CFT, as mandated by FATF and Curaçao regulations. Our comprehensive Business Risk Assessment (BRA) identifies and evaluates inherent risks across key domains, assesses the effectiveness of controls, and determines residual risk. The following major risk categories have been analyzed: Products & Services, Customer Base, Delivery Channels, Geographic Exposure, Transaction Flows, Technology Infrastructure, and Human Factors. For each category, the BRA assigns a risk rating (Very Low to Very High) before and after mitigation:

- *Inherent Risk:* Online casino and sports betting services carry high inherent ML/TF risk due to potential misuse of gambling to launder illicit funds, non-face-to-face onboarding, and global reach. For example, a diverse global customer base increases the chance that some users could be high-risk (e.g. PEPs or criminals).
- *Mitigation Measures:* Trendy Games implements robust controls to mitigate these risks, including strict Know-Your-Customer (KYC) procedures, automated transaction monitoring, geo-restrictions blocking high-risk jurisdictions, secure technology and cybersecurity measures, employee training, and internal controls.
- *Residual Risk:* After applying controls, most risk categories are reduced to Moderate or Low-Moderate residual risk levels. No uncontrolled high risks remain; all residual risks are within the company's risk appetite and deemed manageable. Notably, the Geographic Exposure category remains the highest residual risk (rated "Moderate-High") due to serving various markets, but this is carefully managed by excluding or restricting certain high-risk regions. The overall residual risk for Trendy Games is rated **Moderate**, reflecting substantial risk reduction through our controls.

Appendix B provides a summary risk matrix of inherent and residual risk ratings with key controls per category, demonstrating how our risk-based approach is applied in practice. Trendy Games will update its BRA and policy at least annually, or sooner upon material changes (e.g. new products or markets), to ensure emerging risks are addressed and the risk assessment remains up-to-date.

Governance, Roles and Responsibilities

A culture of compliance is promoted from the top. The senior management of Trendy Games B.V. are ultimately responsible for AML/CFT compliance, overseeing that adequate resources and internal controls are in place. The Board approves this AML/CFT policy and the BRA, and it receives regular reports on the program's effectiveness.

- **Compliance Officer (CO) / MLRO:** Trendy Games appoints a designated Compliance Officer, who also serves as the **Money Laundering Reporting Officer (MLRO)**. This is a senior management position with authority to act independently. The Compliance Officer/MLRO is responsible for designing and implementing the AML/CFT program and has direct access to customer identification data, transaction records, and all necessary information. Key duties include:
 - Ensuring day-to-day compliance with Curaçao AML/CFT laws, regulations, and this policy. This includes staying informed of updates to NORUT, indicator regulations, and FATF/CFATF guidance.
 - Developing and updating internal AML/CFT procedures and controls (e.g. Customer Acceptance Policy, due diligence processes, monitoring and reporting procedures) in line with the risk-based approach.
 - Reviewing adherence to the policy – conducting or overseeing periodic compliance audits and risk assessments to test the effectiveness of controls.
 - Reporting: Receiving internal reports of unusual or suspicious activities from staff, evaluating them, and filing Unusual Transaction Reports (UTRs) with the Financial Intelligence Unit (FIU Curaçao) as required by NORUT. The MLRO ensures that objective indicators (e.g. threshold triggers) and subjective suspicions are reported promptly.
 - Training: Organizing ongoing AML/CFT training for all relevant personnel (see Training section).
 - Record-Keeping: Maintaining records of all CDD documents, transaction monitoring results, and reports made to FIU. Also, keeping an internal log of all reports (both internal and those filed externally).
 - Acting as liaison to regulatory agencies and the CGA – the MLRO is the primary point of contact for AML/CFT inquiries, examinations, or audits by regulators, and for any law enforcement communication regarding money laundering or terrorist financing.
 - Providing regular reports to senior management/Board on the status of the AML/CFT program, including any compliance issues, significant reports made, and recommended improvements.
- **Management:** Senior managers must support the Compliance Officer in implementing controls and allocate sufficient resources (personnel, technology, budget) to AML/CFT. They should promote a strong compliance culture and are involved in approving high-risk customer relationships (e.g. PEP onboarding) and any decision to terminate relationships for AML

reasons. All department heads (e.g. operations, payments, customer service, IT security) coordinate with Compliance to ensure AML controls are embedded in their processes.

- **Employees and Agents:** Every employee has a duty to remain vigilant for potential signs of ML/TF. Staff must follow all AML/CFT procedures in their daily tasks (such as customer onboarding, processing payments, or handling withdrawals). If any employee detects unusual behavior or transactions that might indicate money laundering or terrorist financing, they are required to promptly report it to the Compliance Officer/MLRO (via the internal reporting procedure) without tipping off the customer. Failure to report or deliberate ignorance of red flags can lead to disciplinary action. Employees are trained to understand the legal prohibition on “tipping off” – i.e. they must not inform a customer that they are under investigation or that a report will be filed.

Trendy Games ensures that the Compliance Officer/MLRO is fit and proper for the role (background checks are conducted and qualifications are verified). The Compliance function operates independently from the business lines to avoid conflicts of interest. Where the company engages third-party service providers or agents (such as affiliates or payment processors) that have customer-facing roles, we will communicate relevant AML/CFT requirements to them and ensure their activities are monitored for compliance with this policy.

Customer Due Diligence (CDD)

Trendy Games B.V. maintains strict Customer Due Diligence (CDD) measures to verify the identity of its players and assess their risks. In line with Curaçao’s National Ordinance on Identification when Rendering Services (NOIS) and the 2025 AML/CFT Regulations, the company does not permit anonymous or fictitious accounts. CDD is performed at the start of the business relationship (onboarding) and on an ongoing basis as needed. The key elements of our CDD program include:

- **Identification and Verification:** All customers must be identified with at least the following information at account registration: full legal name, date of birth, nationality, current permanent address, and a unique identification number (e.g. ID card or passport number). The identity is verified using reliable, independent source documents, data or information – typically a government-issued photo ID (passport, driver’s license, or national ID) and proof of address (such as a utility bill or bank statement) or by utilizing other technological measures, including information obtained from trusted third-party service providers (such as payment institutions). Verification of identity is required before a customer is allowed to deposit or wager beyond minimal limits. According to Curaçao regulations, casinos must perform CDD in specified circumstances, including when a player engages in transactions equal to or above NAf. 4,000 (Netherlands Antillean Guilders). This threshold applies to single transactions or a series of linked transactions that together meet or exceed NAf. 4,000. In practice, Trendy Games applies CDD for all customers upon onboarding, regardless of transaction size, due to the online environment and our risk-based policy. Identification must be completed by the time a cumulative transaction of NAf. 4,000 is reached at the, otherwise the account will be frozen pending verification. If a customer cannot be verified or refuses to provide required information, the account will not be activated (or will be closed) and any pending transactions will be blocked.

- **Purpose and Nature of the Relationship:** At onboarding, Trendy Games gathers information to understand the intended nature of the business relationship. Given the industry, the purpose is typically self-evident (online gambling entertainment). However, we may collect information such as the customer’s occupation or source of funds to ensure their profile and expected activity are reasonable. Higher-risk customers (e.g. high spenders) are asked to provide details on the source of their gambling funds. The overarching goal is to “build a customer profile” that helps in detecting unusual deviations during later account activity.
- **Risk Profiling:** As part of CDD, each customer is assessed for risk and assigned a preliminary risk rating (Low, Medium, or High). Trendy Games uses a structured Customer Risk Assessment (CRA) model (see Appendix A) that evaluates factors such as country of residence, age (must be adult), occupation, PEP status, initial deposit amount, and anticipated gaming activity. For example, a customer from a low-risk country with a modest initial deposit might be Low risk, whereas a customer from a high-risk jurisdiction or a Politically Exposed Person (PEP) will be classified as High risk from the start. The risk rating determines the level of due diligence: High-risk customers undergo Enhanced Due Diligence (see next section). Risk ratings are updated dynamically based on the customer’s actual transaction behavior and any new information or screening hits (this is part of ongoing monitoring). **Appendix A details** the scoring methodology and criteria used in the CRA.
- **Timing of CDD:** Generally, CDD (identification and verification) is completed prior to establishing the account relationship or before any significant transaction is permitted. In situations where verification documents are pending, the account is subject to restrictions (e.g. cumulative deposit limits under NAF. 4,000, no withdrawals) until CDD is completed. If verification cannot be completed within a reasonable timeframe, the relationship will not proceed. CDD is also required whenever there is a material change in the relationship (e.g. suspicion of illicit activity arises, doubt about previously obtained data, or if the customer hits certain thresholds requiring re-verification).
- **Ongoing CDD:** Customer information is kept up-to-date. Trendy Games reviews and refreshes CDD data especially for medium and high-risk customers. For example, a medium-risk customer’s profile might be reviewed every 1–2 years, while a high-risk or VIP customer is reviewed at least annually (or more frequently if warranted). During these reviews, customers may be asked to provide updated documents or clarify changes (e.g. new address or new source of funds if their gambling volume has increased). This ensures that our knowledge of the customer remains current and accurate over time.
- **Refusal and Termination:** If at any point a customer fails to comply with CDD requests, provides false information, or is found to be engaging in activities incompatible with compliance (e.g. attempted use of false identity or proxies), Trendy Games will refuse to open the account or will terminate an existing business relationship. Such cases may be reported to FIU if they meet reporting criteria (e.g. the attempted transaction by an unknown person could itself be an unusual transaction indicator). Likewise, if we determine that continuing a relationship would expose the company to unacceptable ML/TF risk (for instance, if a customer is found to be on a sanctions list or involved in criminal activity), we will end the relationship and, where appropriate, file a report.

Enhanced Due Diligence (EDD) for High-Risk Customers

For customers or situations that present a higher risk of ML/TF, Trendy Games applies Enhanced Due Diligence (EDD) measures above and beyond standard CDD. In line with FATF Recommendation 13 and the risk-based approach, EDD is triggered for (but not limited to) the following scenarios:

- **Politically Exposed Persons (PEPs):** Any customer identified as a PEP – including domestic or foreign PEPs, their immediate family members, or close associates – is considered high risk. Upon PEP identification, senior management approval is required to either onboard or continue the business relationship. EDD measures for PEPs include obtaining information on the individual's source of wealth and source of funds for gambling, conducting enhanced ongoing monitoring of their transactions, and subjecting their account to more frequent review. All PEPs are automatically categorized as High Risk in our CRA scoring system (e.g. assigned maximum risk score). If a person is discovered to be a PEP only after onboarding, the same EDD measures apply and a review is immediately undertaken to decide whether to maintain the relationship under stringent controls or to terminate it. (According to CGA regulations, if a customer is identified as a PEP, the casino must implement required measures within 30 days or terminate the relationship.)
- **High-Risk Jurisdictions:** Customers from or connected to high-risk countries (as per our country risk list) are subject to EDD. Trendy Games maintains a list of jurisdictions that are considered high-risk for ML/TF, informed by credible sources: FATF lists of High-Risk Jurisdictions (blacklist) and Jurisdictions under Increased Monitoring (grey list), CFATF advisories, EU high-risk third countries list, UN sanctions, as well as Transparency International's Corruption Perceptions Index. If a player's country of residence or funds origin is in a high-risk jurisdiction, we perform deeper checks: requiring additional identification documents, proof of source of funds, and closer scrutiny of transactions. In some cases, customers from certain prohibited jurisdictions (e.g. sanctioned countries or those with no sufficient AML controls) are not accepted at all – our system will block registrations from those locations. For allowed but high-risk regions, senior management sign-off is needed to approve the account after satisfying enhanced checks.
- **Large or Unusual Transactions / High-Value Players:** Any customer who intends to, or does, transact in large volumes that are inconsistent with a normal player profile will face EDD. For example, a customer who deposits or withdraws amounts far above thresholds, it will trigger enhanced scrutiny. EDD measures may include requesting detailed Source of Funds (SoF) or Source of Wealth (SoW) documentation – such as bank statements, payslips, proof of business income, or other evidence – to substantiate that the funds used for gambling are from legitimate origins. We may also impose lower transaction limits or hold withdrawals until satisfactory information is received. High-value VIP players are reviewed regularly and their accounts are subject to approval by the Compliance Officer.
- **Unusual Account Behavior:** If a customer exhibits patterns that are red flags for potential money laundering, we escalate to EDD. Examples include: playing with minimal or no actual gambling (depositing and withdrawing without significant betting – essentially using the account as a money conduit), sudden changes in betting patterns (a normally small-stakes player suddenly betting or moving large funds), multiple accounts suspected to be linked, or other behavior indicative of “money mule” activity. In such cases, the Compliance team will intervene to investigate the behavior, possibly interview the customer or request additional info, and heighten

monitoring on the account. The risk score of the customer is increased and the account may be flagged for suspicious activity pending a conclusion.

- **Other High-Risk Factors:** Additional scenarios warranting EDD include customers with adverse media hits (e.g. news indicating involvement in financial crime), customers in industries known for high cash turnover or corruption (if known), or complex/unusual business relationships (though our business is retail-focused, if a scenario arose like an agent betting on behalf of others, etc., it would trigger EDD).

Enhanced Measures: When EDD is applied, Trendy Games takes some or all of the following steps, as appropriate to the case:

- Obtaining senior management approval for establishing or continuing the business relationship.
- Obtaining additional identification or verification materials (e.g. a second form of ID, notarized documents, or face verification selfies compared to ID).
- Requiring detailed source of funds/wealth information, and verifying this information to the extent possible (for instance, confirming salary via paystips, or checking corporate ownership for a business owner).
- Conducting more frequent and extensive ongoing monitoring of the customer's transactions (see Monitoring section). High-risk accounts are subject to more stringent rules in our automated monitoring system (lower alert thresholds) h. The Compliance Officer may also conduct manual reviews of high-risk accounts more often.
- Limiting or controlling certain transactions: e.g., not allowing third-party payments, restricting the use of certain high-risk payment methods, or limiting the maximum deposit/withdrawal amounts for the account until comfort with the customer increases.
- Where applicable, performing on-site visits or video conference interviews (though for an online gaming platform this may not apply often, it could be relevant if the customer is a business entity or high-value client where personal interaction aids due diligence).

If EDD measures do not resolve the risk (for example, if a PEP cannot adequately explain their source of wealth or a high-risk customer refuses to provide information), the company will consider terminating the relationship. All decisions and steps taken under EDD are documented. By applying EDD to high-risk situations, Trendy Games ensures compliance with FATF Recommendation 10 (due diligence) and 12 (PEPs), as well as Curaçao's requirement that higher-risk transactions get special attention.

Ongoing Monitoring & Transaction Monitoring

Trendy Games employs continuous ongoing monitoring of customer activity to detect unusual or suspicious behavior promptly. This includes both transaction monitoring (of financial transactions and betting patterns) and periodic screening of customer information against watchlists. Our monitoring process is risk-based, meaning higher-risk customers are monitored with greater frequency and more sensitive thresholds.

- **Automated Transaction Monitoring System:** The company uses an automated monitoring system that aggregates and analyzes transactions (deposits, wagers, winnings, withdrawals) across the platform. The system is configured with rules and scenarios tailored to gaming activities. For example, it will flag if a customer's deposit and withdrawal amounts are nearly

the same with minimal gameplay (a possible indicator of laundering), if there are rapid movements of funds through an account, large single transactions, or unusual spikes in activity. It also checks for structuring (many smaller transactions that in sum exceed thresholds) and unusual patterns like large deposits followed by multiple smaller withdrawals to different payment methods. These rules are calibrated according to risk tier: known high-risk customers have lower thresholds for triggering alerts, meaning even relatively small anomalies will be flagged for review, whereas low-risk customers might only trigger on larger deviations. All alerts generated by the system are reviewed by the compliance analysts or MLRO. Each alert results in either a reasonable explanation (and is closed) or escalation for investigation. Multiple alerts on the same customer will result in an in-depth review of that account's activity.

- **Manual and Ad-Hoc Monitoring:** In addition to automated rules, the Compliance team performs manual monitoring, especially for VIP or high-risk clients. This can include regularly examining high-risk account ledgers, reviewing chat logs or communications if relevant (for signs of collusion or unusual requests), and checking if actual gameplay corresponds to deposits (to catch anyone just cycling money). If any red flags are spotted (such as a customer asking how to withdraw without betting, or references to third-party funding), those accounts are scrutinized.
- **Customer Profile Review:** Ongoing monitoring also involves ensuring transactions align with the customer's known profile. The initial risk profile (from CDD) sets expectations for activity. If a low-risk customer begins to behave like a high-risk one (e.g. a low-income occupation but suddenly gambling very large amounts), the monitoring system will flag this and **the risk rating of the customer is updated** accordingly. The Compliance Officer can adjust a customer's risk level in the CRA based on observed behavior, which may impose EDD measures going forward. This dynamic feedback loop ensures the risk assessment remains current.
- **Link Analysis:** We also monitor for links between accounts (for example, shared devices, IP addresses, or payment instruments) that could indicate collusion, multi-accounting, or syndicate activity. Such links might reveal a network of accounts acting in concert to launder money or circumvent limits. If found, we treat the grouped accounts as higher risk collectively and investigate accordingly.
- **Transaction Approval Triggers:** Certain transactions may require compliance approval before completion. For instance, any single withdrawal above a high threshold (set internally, e.g. €10,000) might be held pending a compliance check of the account's recent activity and CDD status. Similarly, a deposit that is unusually large relative to the customer's profile could be temporarily halted for review. These checkpoints act as an additional safeguard to ensure suspicious transactions are intercepted in real-time when possible.
- **Documentation of Monitoring:** All monitoring actions and decisions are logged in a case management system. If an alert is closed, the analyst records the rationale (e.g., "large win legitimately explains withdrawal"). If escalated, the case file will include the analysis performed, any communication with the customer, and the outcome (report filed or not). This audit trail is essential for internal audit and for demonstrating to regulators the effectiveness of our ongoing monitoring.

Through ongoing monitoring, Trendy Games aims to identify unusual transactions as soon as possible, ensuring that any required reports to FIU can be made in a timely manner and that we swiftly mitigate risks (including account freezes if necessary). The level of ongoing monitoring is always commensurate with the customer's risk: even low-risk customers are monitored, albeit with less sensitivity, since no customer is exempt from oversight. This approach is consistent with FATF Recommendation 10

(ongoing due diligence) and the expectation under Curaçao law that casinos monitor transactions to detect deviations from expected behavior.

Sanctions Screening and PEP Screening

Trendy Games integrates robust sanctions screening and PEP screening into its AML/CFT controls. These processes ensure we do not do business with prohibited persons or entities and that we identify politically exposed persons for enhanced measures:

- **Sanctions Screening:** The company complies with all applicable sanctions laws, including UN Security Council sanctions, EU sanctions regulations, and the Sanctions National Ordinance of Curaçao. Upon account registration and continuously thereafter, we screen each customer's name (and where available, other identifiers like date of birth) against international sanctions lists, such as: UN consolidated sanctions list, EU consolidated list, OFAC SDN list (United States), and any local Curaçao/Kingdom of the Netherlands sanctions lists. If a potential match is found at onboarding, the account is put on hold for verification of the match. Under no circumstances will Trendy Games knowingly establish or continue a business relationship with a sanctioned individual or entity. A confirmed name match to a sanctions list results in the immediate blocking or freezing of the account and funds, and a report to the FIU (since an attempted transaction by a listed person is an unusual transaction that must be reported). Our internal procedures include a "sanctions hit escalation" workflow to rapidly confirm matches (using additional data or requesting info from the customer if needed, without tipping them off to the reason for the query). We also screen for any ownership or control by sanctioned parties (for example, if we ever had corporate customers or if we detect an individual is acting on behalf of a sanctioned entity).

Ongoing screening is performed at least daily – our systems re-check the entire customer base whenever sanctions lists are updated (at minimum once every 24 hours). This ensures that if a customer becomes sanctioned after onboarding, we quickly identify it. In such cases, the same freeze-and-report procedure applies. Additionally, any transaction involving certain high-risk jurisdictions or counterparties (e.g. withdrawal to a bank in a sanctioned country) would be flagged for investigation.

- **PEP Screening:** As part of CDD and ongoing monitoring, we screen all customers for PEP status. We utilize databases and watchlists (e.g. World-Check, Dow Jones, or similar compliance data providers) that list known politically exposed persons globally. During onboarding, if the customer's name or personal details match a PEP profile, the compliance team is alerted. As required, we then verify whether the individual is indeed the same person (sometimes a common name might trigger a false positive). If confirmed as a PEP, the account is labeled high-risk and EDD procedures are initiated (see EDD section). Senior management approval is needed to onboard a PEP, and if approval is granted, all the special measures for PEPs (source of wealth checks, enhanced monitoring, etc.) are applied. Our policy is generally cautious with PEPs – if the risks associated cannot be mitigated to a satisfactory level, we may choose not to onboard the PEP or to terminate the relationship if discovered later.

We rescreen existing customers regularly for PEP status changes. A customer who was not a PEP at onboarding might become one (for example, if they attain a political office). Our nightly screening would catch this, and we would then treat the account as high-risk going forward. We also screen for close associates and family members of PEPs as far as data is available. If a customer is found to be closely connected to a PEP (but not a PEP themselves), we also consider applying EDD on that basis.

- **Adverse Media Screening:** In addition to formal sanctions/PEP lists, we monitor for any adverse media on our customers that might indicate involvement in crime or terrorism. The Compliance Officer may perform internet searches or use screening tools to check if a customer's name appears in news relating to financial crime, fraud, terrorism, etc.. If significant negative news is found, the customer's risk rating can be raised and their activity closely reviewed. In severe cases (e.g. a customer is named in a law enforcement investigation for money laundering), we may suspend the account pending further due diligence or choose to exit the relationship.

Screening Records and Frequency: All screening results and any follow-up actions are documented. The lists used (sanctions/PEP lists) are updated in real-time via our screening provider. Employees are trained to recognize potential sanctions or PEP matches and to immediately inform Compliance if they encounter any during manual processes. Trendy Games ensures screening is not a one-time event but an ongoing process integrated with customer onboarding, transaction processing, and periodic reviews.

By conducting thorough sanctions and PEP screening, Trendy Games adheres to Curaçao's legal requirements (e.g. compliance with the Sanctions National Ordinance) and FATF Recommendations 6 and 7 (targeted financial sanctions related to terrorism and proliferation financing). Any **hits leading to blocked accounts are reported to the FIU** as unusual transactions per the indicator regulations.

Record-Keeping and Data Retention

In compliance with Curaçao law and FATF Recommendation 11, Trendy Games maintains a comprehensive record-keeping system for all documents and information obtained through CDD, as well as records of transactions and reports made. Our record-keeping policy includes:

- **Customer Identification Records:** All copies of identification documents, verification materials, address proofs, source of funds information, and risk assessments for each customer are securely stored (electronically in our KYC system). These records are retained for at least **5 years after the end of the customer relationship** or the date of the occasional transaction, whichever is later. This retention period meets or exceeds the minimum required by NORUT and related regulations. In practice, given the long-term nature of online accounts, records are kept throughout the active period of the account and the 5-year clock starts upon account closure. If required by law or regulatory instruction (e.g. in case of ongoing investigations), records may be kept longer.
- **Transaction Records:** We keep detailed records of all financial transactions conducted by customers on the platform. This includes deposits, withdrawals, bets/wagers, wins, transfers (if any between products), etc. Each transaction record typically contains date, amount, currency, involved account(s), and method (e.g. credit card, e-wallet, bank transfer). These transaction logs are maintained in our databases and can be retrieved and provided to authorities upon

request. As per legal requirements, transaction records are also kept for at least 5 years. These records enable us to reconstruct a complete audit trail for a customer's activity, which is crucial in the event of an investigation.

- **Due Diligence and Monitoring Records:** Any analysis, findings, and conclusions from enhanced due diligence reviews or ongoing monitoring (alert investigations) are documented and stored. For instance, if we conducted a source of wealth inquiry on a high-risk customer, the documents provided and the internal memo of the outcome are saved to that customer's compliance file. Similarly, if an alert was triggered and investigated, the case notes and resolution (including rationale for whether or not to report) are recorded in our case management system. These ensure we have evidence of compliance actions and decision-making processes.
- **Reporting Records:** Copies of all **Unusual Transaction Reports (UTRs)** filed with the FIU are kept internally (usually the PDF or form confirmation from the goAML reporting portal, or at least the reference number and details of the report). We also maintain an internal log of all internally raised suspicious activity reports from staff and what action was taken. This log helps in tracking the pipeline from detection to filing (or decision not to file). We keep these reporting records for at least 5 years from the date of report. Additionally, any correspondence with the FIU or law enforcement (e.g. if they ask for follow-up information) is retained.
- **Training Records:** We document all AML/CFT training sessions delivered, including dates, topics, and attendee lists (signed or acknowledged by employees). Training materials (presentations, handouts) are archived. This evidences our compliance with training obligations and can be shown to regulators. Training records are generally kept for a minimum of 5 years as well.
- **Data Security:** All records are maintained in a secure manner to preserve confidentiality. Electronic records are protected by access controls – only authorized Compliance staff and other need-to-know personnel can access sensitive KYC files. Physical records (if any) are stored in locked cabinets in restricted areas. We also comply with applicable data protection regulations when handling personal data. However, AML laws permit retention and sharing with authorities notwithstanding privacy laws.
- **Auditable and Accessible:** Records are kept in a format that is readily accessible and searchable so that we can promptly respond to any official request from regulators, the FIU, or other competent authorities. For example, if the FIU requests all transactions of a customer or a copy of their ID, we can retrieve and provide those without delay.

This rigorous record-keeping ensures that Trendy Games can provide evidence of compliance and effectively assist in any investigations of financial crime. It also fulfills the obligations under Curaçao's AML/CFT framework (which mirrors FATF's requirement of retaining identification data, account files, and business correspondence, as well as transaction data, for at least five years).

Internal Controls and Independent Audit

Trendy Games B.V. has established a system of internal controls, policies, and procedures to ensure that the AML/CFT program is effectively implemented and that the company complies with all requirements. This AML/CFT Policy itself is a primary internal control document, supplemented by more detailed procedural manuals and checklists for operational staff. Key aspects of our internal control framework include:

- **Policy Governance:** This policy is approved by the Board and is communicated to all relevant staff. It will be reviewed on a regular basis (annually, or more frequently if needed) to incorporate any changes in laws, regulations, or business operations. Updates to the policy must also be approved at the appropriate senior level. The Compliance Officer is responsible for proposing updates and ensuring implementation of approved changes.
- **Procedures and Guidelines:** Detailed **Standard Operating Procedures (SOPs)** support this policy. For example, we have written procedures for customer onboarding KYC steps, verifying documents, conducting risk scoring, handling matches from screening, investigating transaction monitoring alerts, and filing FIU reports. Employees are trained on these procedures and they are accessible in our internal knowledge base. The procedures are also aligned with the latest regulatory guidance (such as the CGA's AML Guidance for casinos).
- **Segregation of Duties:** Wherever practical, we segregate key duties to prevent conflicts or single points of failure. For instance, the staff who approve payouts cannot add new payment methods without additional oversight, and those who process customer registrations are not solely responsible for their risk rating assignment (Compliance reviews high-risk classifications). This helps prevent collusion or bypassing of controls by any one individual. High-risk decisions (like overriding an alert or deciding not to report something significant) are typically reviewed by at least two people (e.g. MLRO and another manager).
- **Employee Screening:** As part of internal controls, Trendy Games conducts screening of its own personnel (especially those in sensitive roles). New hires in relevant departments undergo background checks, including criminal record checks and reference checks, to ensure integrity (we will not employ individuals with relevant criminal convictions such as fraud or money laundering offenses) gamingcontrol.spin-cdn.com. Existing employees in critical roles are periodically re-screened or required to sign declarations of no convictions. Additionally, all staff must agree to abide by confidentiality and AML compliance standards. This reduces the risk of **insider threats** or negligence.
- **Independent Audit Function:** In line with regulatory expectations gamingcontrol.spin-cdn.com, Trendy Games' AML/CFT program is subject to independent testing. We will engage an independent auditor or internal audit department (if one exists separate from compliance) to review the AML/CFT program at least annually. The audit will assess the effectiveness of our controls, sample test transactions and CDD files, evaluate the adequacy of training, and verify adherence to this policy and procedures. Any findings or recommendations from the audit are reported to the Board and must be addressed by management in a timely manner. This independent review is critical to ensure our program is robust and to identify any gaps or areas for improvement.
- **Compliance Monitoring and Reporting:** Apart from the independent audit, the Compliance Officer conducts ongoing self-assessments and prepares periodic compliance reports. These reports (e.g. quarterly) might include metrics like number of new high-risk accounts, training sessions conducted, number of alerts and STRs (Suspicious Transaction Reports) filed, any compliance incidents, etc. The Board or senior management reviews these, which keeps AML/CFT on the agenda and allows for timely action if issues arise.
- **Incident Response:** We have an internal procedure for responding to AML/CFT incidents. For example, if a significant suspicious matter is discovered (like an internal fraud or a major money laundering case), there are clear steps: immediate escalation to the MLRO and senior management, account freezing if needed, internal investigation, notification to regulators if appropriate, and remediation to prevent future occurrences. The company also has a

whistleblower policy that allows employees to confidentially report misconduct or concerns (including any AML/CFT compliance failures) without fear of retaliation.

- **Compliance with CGA Supervision:** As a licensed remote gaming operator under the LOK, Trendy Games acknowledges the supervisory authority of the Curaçao Gaming Control Board (CGA) for AML/CFT. We will fully cooperate with any inspections, information requests, or examinations by the CGA. The Compliance Officer will act as the liaison during such examinations and ensure that any deficiencies noted by the CGA are corrected swiftly. The CGA has the power to examine our AML program, and this policy is written to meet the CGA's requirements for casino AML programs.

Overall, these internal controls ensure that AML/CFT is integrated into the daily operations of Trendy Games. The tone from the top and a clear framework of policies/procedures support a strong compliance culture. Through independent auditing and regulatory oversight, we continually test and improve our controls to maintain an effective defense against money laundering and terrorist financing risks.

Training and Awareness

Trendy Games B.V. implements a comprehensive AML/CFT training program to ensure that all relevant employees are aware of their obligations and are capable of fulfilling them. Training is a crucial component of an effective AML/CFT regime, as recognized by FATF Recommendations and Curaçao regulations. Our training regimen includes:

- **New Employee Induction:** All new hires in relevant positions (customer support, finance, payouts, compliance, management of gaming operations, etc.) receive AML/CFT training as part of their onboarding. This induction training covers the basics of money laundering and terrorist financing, the importance of AML/CFT for our industry, an overview of laws (NORUT, indicator regulations) and internal policies, and the employee's specific responsibilities (such as how to verify an ID or how to escalate a suspicious behavior). New staff are typically trained within their first weeks of employment before they begin handling any transactions or customers independently.
- **Ongoing Annual Training:** The company provides mandatory annual refresher training to all staff involved in AML-relevant activities. This training reinforces key concepts and updates employees on any changes in laws or internal procedures. Annual training is tailored to job functions: e.g., front-line customer support gets practical guidance on KYC document checks and recognizing red flags in customer communications; finance teams learn about transaction red flags and how to handle requests that might be unusual; the MLRO team may attend more advanced training or conferences. A record is kept of completion to ensure everyone attends. The goal is to keep knowledge current and not let awareness fade over time.
- **Targeted Training / Role-Specific:** Certain roles require specialized training. For instance, the Compliance Officer and any deputies will pursue professional development such as external AML certifications (e.g. ACAMS) and stay abreast of typologies and regulatory expectations. The MLRO may also train with FIU programs or workshops by the CGA. Similarly, IT staff who develop our monitoring systems might get training on AML transaction patterns to better understand system requirements. Senior management and the Board are briefed on AML/CFT at least annually so that they understand the risks and the framework in place (this can be in the

form of a management seminar by the Compliance Officer covering the BRA results and any regulatory developments).

- **Training Content:** Our training covers:
 - *Understanding ML/TF:* How money laundering and terrorist financing work, stages of money laundering, specific vulnerabilities in gambling (e.g. chip cash-outs, minimal play).
 - *Legal Requirements:* An explanation of Curaçao's AML laws (NOIS, NORUT) and what they require from casinos and employees – for example, the duty to identify customers, the duty to report unusual transactions, and legal penalties for non-compliance. We highlight the objective indicators like the NAf. 4,000 threshold for reporting and the ban on tipping off.
 - *Policies and Procedures:* Review of internal policies (this document) including how to do CDD, how to escalate suspicious activity, record-keeping rules, and sanctions/PEP processes.
 - *Red Flags:* Concrete examples of suspicious activities or signs of problem gambling behavior that could indicate ML/TF – for instance, multiple accounts, sudden changes in betting, use of multiple credit cards, reluctance to provide KYC documents, etc. Staff are taught to be vigilant for these and to react according to procedure.
 - *Case Studies:* We often include case studies, possibly anonymized real cases from the industry or our own incidents, to illustrate how a suspicious pattern was identified and handled. This helps make the training more relatable and memorable.
 - *Testing and Feedback:* After training sessions, we may use quizzes or tests to gauge understanding. Any gaps identified lead to follow-up clarifications.
- **Employee Acknowledgment:** Employees are required to acknowledge their understanding of the AML/CFT policy and their obligations (usually by signing an acknowledgment or via an e-learning system completion). This creates personal accountability.
- **Continuous Awareness:** Beyond formal training sessions, we maintain AML awareness through periodic communications – e.g., compliance newsletters, infographics on bulletin boards (or intranet) summarizing key red flags, and instant updates if a new scam or typology emerges that staff should know about. The Compliance Officer might disseminate FATF or CFATF alerts about new trends or CGA advisories to all relevant staff.
- **Training for Third Parties:** If we have agents or partners directly involved in player interactions (like an affiliate with direct contact or a white-label arrangement), we ensure those persons are also given appropriate training or at least the guidance to meet our standards.

An effective training program ensures that AML/CFT is not just a matter of written policies but is ingrained in the daily practices of our team. Well-trained staff act as the first line of defense against suspicious activities and help create an environment where attempting to launder money through FridayBet.com is difficult. We periodically evaluate the training effectiveness (e.g., through the internal audit or by monitoring if fewer mistakes occur in KYC processing) and update the program as needed. All training activities are documented as part of our compliance records.

Reporting of Unusual Transactions and Suspicious Activity

As a registered service provider under the NORUT (National Ordinance on the Reporting of Unusual Transactions), Trendy Games is legally obligated to report unusual transactions to the Financial

Intelligence Unit of Curaçao (FIU Curaçao). Our policy is to comply fully with all reporting requirements. The reporting regime includes both objective indicators (specific threshold-based or list-based triggers) and subjective indicators (transactions that we suspect to be related to ML or TF). Key points of our reporting procedure:

- **Internal Reporting (Detection to MLRO):** All employees must promptly notify the Compliance Officer/MLRO if they observe any transaction or activity that is unusual or potentially suspicious. We have an internal form and secure channel for this purpose. For example, if a customer service agent notices a player asking unusual questions about payout structuring, or if a payments analyst sees a deposit pattern that doesn't make economic sense, they report it internally. The MLRO will log the report and begin an investigation. Employees are reminded that reporting internally is both an obligation and protected (no retaliation for good-faith reports). They are also reminded not to tip off the customer – meaning they should not inform the customer of their suspicion or that they are being reported.
- **Assessment by MLRO:** The Compliance Officer/MLRO (and team) will evaluate internal reports alongside any alerts from our monitoring systems. This may involve reviewing the customer's full activity, checking their KYC details again, performing open-source intelligence (web searches), and perhaps querying the customer for additional information if needed and if it won't tip them off. The MLRO will decide whether the activity qualifies as an "unusual transaction" under the law, which then must be reported to FIU. Many unusual transactions will fall under defined indicators, but even if not, any suspicion of ML/TF means it must be reported under the subjective indicator.
- **Objective Indicators (Automatic Triggers):** Curaçao's Regulation Indicators of Unusual Transactions provides specific scenarios that are deemed unusual and must be reported regardless of any subjective assessment. For the gaming sector (casinos, including online), the relevant objective indicators include:
 - **Large Transaction Threshold:** Any transaction (or series of linked transactions) in the amount of NAf. 4,000 or more is considered unusual. Trendy Games will treat any single deposit or withdrawal $\geq$ NAf. 5,000 as a reportable unusual transaction. Also, multiple smaller transactions that appear linked and together meet or exceed NAf. 5,000 (e.g. 5 deposits of NAf.1,000) are aggregated and reportable. Our systems help detect such structuring.
 - **Sanction List Hit:** Any proposed or conducted transaction involving a person or entity on a sanctions list (per the Sanctions National Ordinance) is an unusual transaction that must be reported. This aligns with our earlier sanctions screening – if we ever find a customer is on a relevant sanctions list or an attempted transaction would violate sanctions, we not only block it but also report it to FIU as an unusual event. (For instance, a withdrawal request to a bank in a sanctioned country, or an account registration by a blacklisted terrorist financier, would trigger a report even if no money was actually paid out.)
 - **Law Enforcement Inquiry:** A transaction that is reported to police or justice authorities in connection with ML/TF is itself an indicator for FIU reporting. This typically means if we, for some reason, have already engaged law enforcement about a transaction (or they have inquired with us), we must also file an FIU report.
- **Subjective Indicator (Suspicious Activity):** Aside from the above objective triggers, any transaction or activity for which we have a suspicion of money laundering or terrorist financing

must be reported. This is often referred to as a Suspicious Activity Report (SAR) or UTR under subjective grounds. This could be any number of scenarios: e.g., a customer's pattern of play strongly suggests they are layering funds, or their documents appear falsified and we suspect identity fraud for ML purposes, or the customer tries to circumvent our controls (like using multiple accounts). The threshold here is "reason to assume" the transaction could be related to ML/TF. The MLRO uses judgment, but errs on the side of reporting if in doubt. We understand that under NORUT we are protected by law when reporting in good faith, and that it is mandatory to report suspicions. The FIU may later determine if it's truly suspicious or not, but our duty is to report unusual/suspect activities without delay.

- **Reporting Process to FIU:** When an unusual transaction is identified, the MLRO will compile all relevant details (customer info, transaction details, and why it's unusual) and submit a report electronically. Each report is assigned a unique reference. We aim to file reports as quickly as possible after detection. Curaçao law requires prompt reporting; while it does not specify an exact number of days in this text, in practice reports are expected without undue delay (often within 14 days of determining the activity is unusual, and sooner for very serious matters). Our internal target is to report within 5 business days of confirming the need to report (and within 24 hours for critical sanctions-related hits). We prioritize these to ensure compliance. If we are still investigating but suspect strongly, we may report preliminary information and update later if needed, rather than delay a filing.
- **Post-Reporting Actions:** Once a report is filed, we do not inform the customer (no tipping off). We may, depending on the situation, continue monitoring the account extra carefully. If the reported issue is serious (e.g. clear criminal activity), we might choose to freeze or close the account after consulting with FIU or as per legal allowances. The law prohibits tipping off the customer that a report has been made. Our staff are trained in this non-disclosure. If law enforcement needs further info, we cooperate, but within the company knowledge of the report is kept strictly confidential (need-to-know basis).
- **Reports to Law Enforcement:** We understand that FIU Curaçao will analyze our unusual transaction reports and, if they conclude there is indeed suspicion of ML/TF, they will forward them to the Public Prosecutor's Office as suspicious transactions for possible criminal investigation. We do not have to make that determination ourselves; we focus on reporting unusuals to FIU. However, if we ever directly identify a crime in progress or immediate threat (like knowledge of terrorist activity), nothing in this policy prevents us from alerting law enforcement directly as well, in addition to filing with FIU.
- **Statistics and Trend Analysis:** The MLRO maintains statistics of all reports made. Periodically, we analyze these to see if there are any trends (for example, multiple reports arising from a particular country or game type) which might inform adjustments in our risk controls. We also review any feedback from the FIU. If FIU or CGA issues typologies or red flag guidance, we incorporate that into training and monitoring rules.

Appendix A: Customer Risk Assessment Model (CRA)

Trendy Games employs a quantitative Customer Risk Assessment (CRA) model to assign each customer a risk score and rating (Low/Medium/High) at onboarding and through the customer's life cycle. This model aligns with the risk factors identified in the BRA and ensures a consistent, documented risk-based approach to CDD. The main components of the CRA model include:

Risk Factors Evaluated:

- **Geography (Country Risk):** Based on the customer's country of residence (and nationality, if different). Countries are categorized by risk level:
 - Low-Risk Country – e.g. EU member states, UK, Canada, Japan (strong AML regimes, low corruption) score low points.
 - Medium-Risk Country – e.g. some Eastern Europe, Latin America or Southeast Asia countries with moderate AML controls score mid-range points.
 - High-Risk Country – e.g. FATF-listed jurisdictions under increased monitoring, or known high-corruption/high-crime areas (examples: Russia, Nigeria, Pakistan, etc., if these are not outright prohibited) score high points.
 - **Prohibited Countries:** If a country is on our prohibited list (very high risk or sanctions), the customer is not onboarded at all. (Thus, in scoring terms, that would be an automatic rejection rather than a numeric score.)
- **Customer Profile and Occupation:** The nature of the customer's occupation or source of income where known:
 - Politically Exposed Person (PEP) – automatically categorized as High risk. In scoring, a PEP gets the maximum risk points (e.g. 5 points), and triggers EDD.
 - High-Net-Worth Individual with unclear income – e.g. a purported businessman or self-employed person depositing very large sums without clear source. This would be high risk (e.g. 4 points) unless documentation of legitimate source is provided.
 - Regular/Salaried Profession – e.g. teacher, engineer, or retiree with an evident steady income. Such a profile is lower risk (e.g. 1 point) as long as their gambling activity is proportionate.
 - Unemployed/Student with significant gambling funds – that mismatch raises risk (high points) because the source of funds is questionable.
 - If occupation is not collected, we infer risk from other information, but generally lack of information means we cannot give benefit of the doubt; if a customer later shows high spending, we will request occupation/source info.
- **PEP/Sanctions/Adverse Media Status:**
 - PEP status: as noted, any PEP is high risk by default.
 - Sanctions list: if a customer is on a sanctions list, they are rejected (no score, just not accepted).
 - Adverse media: if our screening finds serious adverse news (e.g. linked to fraud or crime), we manually increase their risk score or even refuse onboarding.
- **Initial Deposit Amount / Anticipated Account Activity:** We gauge the expected account volume.
 - If the initial deposit (or expected first deposit) is small (e.g. < €1,000), that's low risk contribution.

- Moderate first deposit (€1,000–€5,000) is medium risk.
- Very large first deposit (> €5,000) is high risk. We note large upfront deposits as potential warning unless justified (e.g. a known VIP with verified wealth).
- Similarly, if during registration the customer indicates any expected high level of play, we account for that.
- **Ongoing Transaction Volume:** As the relationship progresses, the monthly turnover (deposits or betting volume) influences risk:
 - If a customer’s monthly throughput stays under, say, €5,000, it’s low risk.
 - €5k–€20k monthly is medium.
 - Exceeding €20k monthly is high risk.
 - Sudden changes (like a spike one month) will prompt a risk re-evaluation.
- **Account and Betting Behavior:** The qualitative patterns of how the account is used:
 - Low Risk Behavior: Regular gambling patterns consistent with entertainment (e.g. placing bets, sometimes losing, sometimes winning, normal variation, with reasonable pauses, etc.).
 - High Risk Behavior: Indicators such as “minimal play” (the customer deposits and quickly withdraws most funds without proportional play), consistently hedging bets or colluding (like betting both outcomes to guarantee minimal loss), using the account in a way that looks like a money service (not a player). Such behaviors flag the account as high risk.
 - Use of multiple accounts or trying to circumvent limits is also high risk.
- **Payment Methods Used:** The types and variety of payment instruments:
 - A single, personal bank account or major credit card in the customer’s own name is considered lower risk (very traceable).
 - If a customer uses numerous different cards, multiple e-wallets, or frequently changes payment methods, that behavior is higher risk. It could indicate attempts to obscure source of funds or involve third parties.
 - Use of any **high-anonymity methods** (for example, prepaid vouchers or gift cards purchased with cash) is considered high risk. (Note: Trendy Games in practice does not allow funding from completely anonymous methods; any attempt to do so is flagged and investigated.)
 - Deposits from accounts not in the player’s own name are generally not allowed; if discovered, it’s a serious risk indicator (could mean third-party funding).

Each risk factor is assigned a point value according to the customer’s circumstance. We maintain a risk scoring matrix where, for instance, Low risk attributes = 1 point, Medium = 3 points, High = 5 points (as an illustrative scheme). Some factors may be weighted more heavily than others. For example, being a PEP or on a high-risk country list carries a high point weight that alone can push the customer into High risk category.

Risk Scoring and Classification: After inputting all relevant factors, the points are summed to an overall risk score. We then classify the customer’s risk:

- 0–5 points = Low Risk,
- 6–10 = Medium Risk,
- 11+ = High Risk (thresholds are set in our model and can be adjusted based on calibration).

This means a customer with all low-risk attributes would score low, whereas any combination of multiple high-risk traits (e.g. high-risk country + large deposits + unusual behavior) would result in a high score. Certain conditions can automatically elevate someone to High risk regardless of numeric score (for instance, if they are a PEP, we treat them as High risk even if other factors are low). The scoring is a tool to guide consistency, but Compliance has discretion to override or manually adjust a risk rating if justified (documenting the reasoning).

Below is a simplified illustration of risk criteria examples at low vs high extremes:

Risk Factor	Low Risk Example	High Risk Example
Geography	Resident of a low-risk country (e.g. Canada or Netherlands)	Resident of a high-risk country (on FATF lists)
Customer Profile	Non-PEP, clear salaried job	Politically Exposed Person (government official)
Initial Deposit	Modest first deposit (e.g. €200)	Very large first deposit (e.g. €20,000)
Monthly Turnover	< €5,000 per month in bets/deposits	> €20,000 per month in bets/deposits
Account Behavior	Regular play, losses and wins in line with entertainment	Mainly deposits & quick withdrawals, little gameplay
Payment Methods	Single credit card in own name	Multiple cards/e-wallets, or use of prepaid vouchers

Risk-Based Actions: The customer's risk rating determines the level of due diligence and monitoring:

- **Low-Risk Customers:** They undergo standard CDD (ID verification) and are subject to normal monitoring. No extraordinary measures, but they are still screened and monitored by automated means routinely. We may do random spot checks on some low-risk accounts as a quality control.
- **Medium-Risk Customers:** These may face slightly enhanced measures, such as additional verification of certain information or source of funds if their activity increases. We review medium-risk accounts periodically (e.g. at least every 12–24 months) to see if their risk has changed. Their transactions might trigger alerts at somewhat lower thresholds than low-risk ones.
- **High-Risk Customers:** These undergo Enhanced Due Diligence (EDD). We require more information (source of wealth documents, etc.), as described in the EDD section. Senior management approval is needed to continue dealing with them. High-risk accounts are reviewed more frequently (at minimum annually, often 6-month intervals). We apply stricter transaction monitoring rules – even small deviations can trigger alerts for high-risk individuals. For example, a €5,000 withdrawal might prompt a review for a high-risk customer whereas for a low-risk customer the threshold might be higher. All PEPs are automatically treated as high-risk with dedicated oversight.

Ongoing Risk Updates: The CRA is not a one-and-done scoring. It updates with new information:

- We rescore customers based on their ongoing activity. The transaction monitoring system can feed risk metrics (like total volume, velocity of transactions) into the risk score dynamically.

- Periodic re-screening (for sanctions/PEPs) may introduce new risk factors (e.g. a customer becomes a PEP).
- If a customer's risk increases (score goes from medium to high), the system/Compliance will adjust their status and enforce appropriate EDD measures (and possibly a re-review of their profile).
- Conversely, if a high-risk customer's activity significantly changes or they provide clarifications that mitigate risk, we may downgrade their risk rating – though cautiously and only after time has passed with no issues.

The CRA model is documented and periodically validated. We ensure the criteria reflect actual risk outcomes and adjust scoring or thresholds if we find too many false negatives/positives. This model helps allocate our compliance resources efficiently: focusing the most attention on those customers who pose the greatest risk, in line with the risk-based approach principle of FATF.

(See Appendix B for how the customer risk ties into the broader business risk controls, and Appendix C for regulatory triggers that override any risk level.)

Appendix B: Risk Matrix – BRA Summary of Risk Categories

The table below summarizes the key risk domains from Trendy Games' Business Risk Assessment (BRA), their inherent risk levels, residual risk after controls, and examples of control measures. This matrix demonstrates alignment between our BRA findings and the controls described in this AML/CFT policy:

- **Products & Services Risk:**
 - *Inherent Risk: **High (4/5)***. Online gambling products (sports betting, casino games) inherently carry high ML risk due to substantial funds turnover and potential misuse (e.g. using betting to mask illegal funds). There is also inherent fraud risk (e.g. chip dumping, bonus abuse) and no crypto is allowed which actually reduces some risk (crypto could add anonymity, so fiat-only keeps risk slightly lower).
 - *Key Controls:* Account-based play only (no anonymous bets); mandatory KYC for all players; monitoring of betting patterns to catch anomalies; limits on bet sizes and withdrawals to detect out-of-norm behavior; use of audited, fair game software to prevent manipulation.
 - *Residual Risk: **Moderate (2/5)***. After these controls, the risk of undetected ML through products is significantly reduced. Regular play is separated from purely financial transactions, making laundering more difficult.
- **Customer Risk:**
 - *Inherent Risk: **High (4/5)***. A global customer base means we may encounter PEPs, criminals, or individuals with illicit wealth. Without controls, the diversity of customers and potential for some bad actors make this high risk.
 - *Key Controls:* Rigorous ID verification of all customers; comprehensive PEP and sanctions screening at onboarding and ongoing; risk-based customer profiling (CRA) to apply EDD to high-risk customers (e.g. source of funds for high rollers, EDD for PEPs). High-risk customers require senior management sign-off. We also enforce a single account per person policy to prevent evasion.
 - *Residual Risk: **Moderate (2/5)***. With thorough KYC and screening, most illicit actors are kept out or identified early, and the majority of legitimate customers pose only moderate risk. The remaining risk is mitigated by ongoing monitoring and the ability to swiftly report suspicious customers.
- **Delivery Channels Risk:**
 - *Inherent Risk: **High (4/5)***. Our services are offered remotely (internet platform) with non face-to-face customer interaction. This raises risk of identity fraud, anonymous access, and use of intermediaries (like someone could create accounts for others). Also, global reach via the internet increases exposure to various risks.
 - *Key Controls:* Implementation of advanced electronic KYC verification (including biometric or liveness checks) to confirm customer identity remotely; **Geo-blocking** of access from prohibited regions; device fingerprinting and other tech to detect multiple accounts or proxy usage; stringent affiliate due diligence (ensuring our marketing channels don't introduce unchecked users).
 - *Residual Risk: **Moderate (3/5)***. We have reduced a lot of the digital channel risk through technology, but some residual risk remains due to the inherently remote nature. This is somewhat higher than other residual risks because no matter what, online onboarding can

never be as certain as face-to-face. However, our controls like KYC and geo-restrictions have lowered it to an acceptable level.

- **Geographic (Country) Risk:**

- *Inherent Risk: **Very High (5/5)***. By potentially serving players worldwide, there's a risk of including high-risk jurisdictions (areas with poor AML controls, high corruption, or terrorism presence). Different countries pose different levels of ML risk, and some may be sanctioned.
- *Key Controls:* Strict **prohibited countries list** – we do not accept registrations from FATF-identified high-risk jurisdictions, sanctioned countries, or other blacklisted regions. Country risk scoring for all allowed jurisdictions; enhanced checks for medium-risk countries (e.g. require proof of address or source of funds for residents of certain nations). Continuous monitoring of geopolitical risk changes (if a country's risk status worsens, we adapt quickly). Transactions are also screened for any flows to/from risky locations.
- *Residual Risk: **Moderate-High (4/5)***. Despite blocking the worst jurisdictions, we still operate in a wide range of countries, some of which carry elevated risk. This remains our highest residual risk area as noted in the BRA. We manage it with tailored controls and watch it closely, expecting it to further decrease as we refine country-specific measures.

- **Transactions/Payments Risk:**

- *Inherent Risk: **High (4/5)***. The platform processes large volumes of transactions through various channels (credit cards, bank transfers, e-wallets). Inherent risks include **structuring** (breaking up transactions to avoid detection), rapid in-and-out movements (laundering or fraud), and payment fraud (stolen cards, chargebacks). Also cash is not directly handled in online, which reduces some risk vs. land-based, but still high.
- *Key Controls:* **Automated transaction monitoring system** analyzing deposits/withdrawals patterns in real time; enforced use of same-name accounts (withdrawals can only go back to the source account in the customer's name) to prevent third-party payments; deposit and withdrawal limits based on risk level; strong fraud detection tools (address verification, 3D-Secure for cards, etc.) to prevent use of stolen payment methods. All transactions $\geq$ NAf.5,000 are automatically flagged (and will be reported per regulations).
- *Residual Risk: **Moderate (2/5)***. With comprehensive monitoring and strict payment policies, the likelihood of undetected suspicious transactions is greatly lowered. We quickly catch unusual transaction behavior and have processes to intervene (e.g. hold funds, request info, report to FIU). Fraud is also curtailed by our controls, protecting the integrity of transactions.

- **Technology & Cybersecurity Risk:**

- *Inherent Risk: **High (4/5)***. As an online service, we could be targeted by cyber-attacks that might compromise data or funds (e.g. hackers inserting malware to alter transactions). Also, system vulnerabilities could be exploited to bypass controls.
- *Key Controls:* A robust cybersecurity program: firewalls, intrusion detection systems (IDS), encryption of data in transit and at rest, regular penetration testing, DDoS protection to keep the site secure, secure software development practices (code reviews, patch management), and an incident response plan for any breaches. Access to sensitive systems is restricted and logged. We also monitor for unusual system activity which might indicate internal misuse.

- **Residual Risk: Moderate (2/5).** While cyber risk can never be entirely eliminated, our strong defenses and vigilant monitoring greatly reduce the risk of a successful attack or unauthorized system abuse. We remain aware that threats evolve, so we constantly update our tech defenses. The residual risk is considered acceptable and is largely about remaining vigilant.
- **Human Factors (Internal Risk):**
 - **Inherent Risk: Moderate (3/5).** This covers the risk of human error or malicious insiders – employees or contractors could fail to follow procedures or could collude in wrongdoing (e.g. accepting a bribe to approve a fraudulent withdrawal). Given we are a relatively small team with a compliance focus, we judge inherent risk as moderate (not as high as other areas, but not negligible).
 - **Key Controls: Training and a compliance-oriented culture** emphasize doing the right thing. Thorough employee screening at hiring (criminal background checks, reference checks) to avoid hiring high-risk individuals. Segregation of duties and dual-control in critical processes reduce the chance of a single rogue actor causing harm. Regular internal audits and oversight of staff work (e.g. managers review a sample of KYC decisions). A whistleblower policy encourages reporting of any unethical behavior internally.
 - **Residual Risk: Low (1/5).** With these controls, the likelihood of an internal failure or collusion is low. We recognize no system is perfect – there’s always a small chance of a determined bad actor or a mistake – but we believe our multi-layered approach (checks and balances, oversight) minimizes human risk to a low level. We maintain this by continuously fostering integrity and competence among staff.
- **Overall Residual Risk: Moderate.** Taking all categories into account, Trendy Games’ overall residual risk is rated Moderate, as per the BRA. This means that while the nature of online gambling presents high inherent risks, our strong controls have mitigated those to a manageable level that meets regulatory expectations. No residual risk category is “High”; the highest (Geography at 4/5) is under targeted controls. We remain vigilant and proactive in further reducing risks where possible, but the current residual risk profile is within our risk appetite and has been approved by senior management.

This risk matrix is included to demonstrate that the measures in our AML/CFT Policy directly address the risks identified in our BRA. The alignment ensures a coherent risk-based approach where resources and controls are commensurate with the level of risk in each area.

Appendix C: Regulatory Thresholds & Reporting Triggers

The following summary outlines important threshold amounts and triggers for AML/CFT actions as defined by Curaçao’s laws and regulations (notably the **Regulation Indicators of Unusual Transactions**, including the 2024 amendments). Trendy Games incorporates these triggers into its procedures:

- **Customer Identification Threshold – NAf. 4,000:** Curaçao’s AML regulations for gaming (NOIS/LID and the 2025 AML/CFT Regulations) mandate that Customer Due Diligence (identification & verification) must be conducted when a player performs a transaction or series of linked transactions totaling **NAf. 4,000** or more . In other words, NAf. 4,000 (approximately USD 2,200 or EUR 2,000) is a key threshold beyond which the casino must have identified and

verified the customer. Transactions can be cumulative (e.g. 4 deposits of NAf.1,000 each would trigger CDD). If a customer hits this threshold and CDD hasn't been completed yet, the account must be frozen to complete verification. Trendy Games' policy is stricter – we aim to complete CDD on all customers at onboarding, before they ever reach this threshold. But this NAf.4,000 rule is noted and complied with as an upper limit in edge cases.

- **Unusual Transaction Reporting Threshold** – NAf. 5,000: As per the indicator regulations for casinos, any single transaction or series of related transactions with a value of NAf. 5,000 or more must be reported to FIU as an unusual transaction. This threshold applies to all forms of transaction (cash, non-cash, electronic, etc.). For online operations, this typically means:
 - A deposit of NAf.5,000 or above into a player account.
 - A withdrawal of NAf.5,000 or above from a player account (including payout of winnings).
 - Purchase of gaming credits or chips worth NAf.5,000 or more (in an online context, converting a deposit into chips is essentially the deposit itself).
 - Multiple smaller transactions that aggregate to NAf.5,000 or more in one gaming session or a short period, if they appear linked.

Trendy Games' system automatically flags when the cumulative value of transactions reaches this threshold and alerts the MLRO to review and prepare a report. **Note:** NAf.5,000 is roughly equivalent to €2,500 or \$2,800 (depending on exchange rates). We also interpret this threshold in other currencies – e.g. if a customer operates in EUR or USD on our platform, we use the equivalent (approximately €2,500 or \$2,800) as the trigger amount.

- **Sanctioned Persons Transactions:** Any transaction involving a person or entity on an official sanctions list (UN, EU, OFAC, or Curaçao's own lists under the Sanctions National Ordinance) is an objective unusual indicator. If we identify that a customer or the beneficiary of a transaction is on a sanctions list, we must report that occurrence. In practice, this could be an attempted deposit or withdrawal by a blacklisted person. Even if our internal policy forbids doing business with them (so we would block it), the mere attempt is reportable. This is why our screening procedures are critical and directly tied to reporting obligations.
- **Suspicious Activity (Subjective):** While not a numeric threshold, it bears repeating that any transaction or activity that we *suspect* to be related to ML/TF is a trigger for reporting (subjective indicator). This is more qualitative – examples include transactions that are unusual with no apparent lawful explanation, structuring below the NAf.5,000 threshold to evade reporting, use of false documents, etc. There is no monetary minimum for suspicion – even a small transaction can be reported if suspicious. Our staff are trained on these red flags and our internal threshold for suspicion is purposefully low: if in doubt, we report.
- **Linked Transactions Definition:** The regulations clarify that separate transactions that appear linked (by same player, in a connected time or manner) should be treated cumulatively for thresholds. For example, if a player breaks a 10,000 deposit into 5 increments of 2,000, that's still $\geq 5,000$ in total and must be reported. Our monitoring is tuned to catch such patterns.
- **Reporting Timeline:** While not explicitly a "threshold," the laws require that once an unusual transaction is identified, it should be reported **promptly**. Guidance often suggests within 14 days at most. Our internal rule is to report as soon as possible, ideally within 5 days of detection (and immediately for something urgent like a sanctions hit). We ensure not to exceed any statutory limit if provided.

- **Currency Equivalents:** NAf. (Netherlands Antillean Guilder) is the legal currency reference. Our platform might use EUR or USD predominantly. We treat the threshold in any currency that equals NAf.5,000. The Compliance team keeps track of exchange rates (NAf is pegged to USD at 1.79 NAf = 1 USD). So effectively: USD ~\$2,793 or EUR ~€2,500 is the magic number for reporting. To be safe, we round down – e.g., we might treat €2,400 or \$2,700 as hitting the threshold given minor fluctuations, to never miss a report.
- **Other Sector-Specific Indicators:** (Informative) The indicator regulation has multiple sections for various sectors. For casinos (including online), we've covered the main points: police-report-related (A), sanctions-list (B), $\geq$ NAf.5k (C) as objective, and the general suspicion as subjective. We are aware of these and have built them into our compliance checklist.
- **Documentation and Appendices Reference:** The full list of indicators is maintained in our compliance manual for reference. We also maintain a threshold table for quick reference by staff (e.g., "Any single withdrawal $\geq$ \$2,800 triggers FIU report"). All unusual reports filed note which indicator they fall under (e.g., "indicator F(C) – transaction $\geq$ NAf.5k" or "subjective indicator – suspected ML").

Summary: In essence, the critical numbers to remember are NAf.4,000 for completing CDD, NAf.5,000 for mandatory reporting, and "any suspicion" as a reason to report regardless of amount. These thresholds from the Curaçao regulatory framework are fully embedded in Trendy Games' AML procedures, ensuring we meet the exact legal standards. By adhering to them, we help protect the business and contribute to the overall integrity of the financial system, while also avoiding regulatory penalties that could arise from non-compliance.

Approved and signed by statutory director Kurason Trust Curacao,
represented by Jonathan Marshal Ruwel Heymans

Date: 7 of April 2025

Signature:

DocuSigned by:

BFFB053659204B9...