



AML & KYC POLICY

*Trickless N.V. (the “**Company**”)*

date	Version	Created	Approved
15 May 2025	V2		

Contents

1. Policy Statement.....	3
2. Purpose and Obligations	3
3. Audience.....	3
4. Definitions.....	3
5. Policy Implementation.....	4
6. MLRO Identification and Contact.....	4
7. Risk Based Approach	5
8. Business Risk Assessment.....	5
9. Risk Management.....	5
Phase 1: Identity Validation and Risk Assessment.....	6
Phase 2: Source Confirmation.....	7
Phase 3: Ongoing Monitoring	8
Phase 4: Destination Confirmation and Verification	10
10. KYC Process	12
Customer Due Diligence (CDD).....	12
Enhanced Due Diligence (EDD)	12
11. Underage Gambling.....	13
12. Jurisdiction and Sanction Lists	14
13. Politically Exposed Persons (PEP).....	15
14. Record Keeping.....	15
15. Reporting	16
16. Training.....	17
17. Compliance and Consequences of Non-Compliance.....	17
18. Policy History.....	18
Appendix A: Measures for the Detection of Money Laundering	18
Appendix B: Live alert triggers.....	20
Appendix C: Reporting Suspicious Activity Policy	21
Appendix D: Procedure for completing SAR.....	23

1. Policy Statement

This Policy applies to all operations under the Curaçao Gaming license. The Company is committed to complying with local anti-money laundering (AML) and counter-terrorism financing (CTF) legislation, including the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the National Ordinance on Identification when Rendering Services (NOIS), as enforced by the Financial Intelligence Unit Curaçao and the Curaçao Gaming Control Board.

2. Purpose and Obligations

The Policy aligns with the regulatory expectations of the Financial Intelligence Unit Curaçao (FIU-Curaçao) and the Curaçao Gaming Control Board (GCB). It ensures adherence to legal obligations and mitigates money laundering risks on Company websites. The Company shall:

1. Appoint and retain a designated Money Laundering Reporting Officer (MLRO).
2. Establish user identity with due diligence before providing services.
3. Retain identification and transactional documents as required by law.
4. Provide initial and ongoing AML/CTF training for staff.
5. Develop and maintain this Policy in line with regulatory obligations.
6. Examine complex transactions likely related to money laundering or terrorist financing.
7. Report any suspicion or knowledge of money laundering/terrorist financing.
8. Ensure adherence to KYC, Enhanced Due Diligence (EDD), and closed-loop transaction policies.

This Policy will be reviewed upon changes to relevant laws/regulations and refresher training will be provided as needed. The MLRO maintains this document.

3. Audience

This Policy applies to all employees, senior management, contractors, and third-party service providers engaged in activities under the Company's Curaçao gaming license. All are expected to comply with AML/CTF obligations.

4. Definitions

- **Money Laundering Reporting Officer (MLRO):** Responsible for implementing and maintaining the AML/CTF framework and reporting suspicious transactions to FIU Curaçao.
- **FIU Curaçao:** Financial Intelligence Unit of Curaçao; responsible for receiving, analyzing, and disseminating reports of unusual or suspicious transactions under NORUT.
- **Curaçao Gaming Control Board (GCB):** Regulatory body overseeing AML/CTF compliance within the licensed gaming sector.
- **Suspicious Transaction Report (STR):** Formal report submitted to FIU Curaçao for suspected criminal proceeds or terrorist financing.
- **Customer Due Diligence (CDD):** Procedures to identify and verify customer identities and beneficial owners,

assess risks, and understand the business relationship.

- **Enhanced Due Diligence (EDD):** Heightened scrutiny for higher-risk customers/transactions, including source of funds/wealth checks and intensified monitoring.
- **Politically Exposed Person (PEP):** Individual holding a prominent public function, their close associates, and immediate family.
- **Unusual Transaction:** Transaction inconsistent with customer profile or lacking clear economic purpose.

5. Policy Implementation

The Money Laundering Reporting Officer (MLRO) is responsible for overseeing the implementation of this AML/CTF Policy, ensuring compliance with all regulatory obligations under Curaçao law. The Company utilizes a risk-based approach, in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the National Ordinance on Identification when Rendering Services (NOIS), to identify and mitigate money laundering and terrorist financing risks.

Policy implementation is maintained through the following core elements:

- **MLRO Oversight:** The MLRO is accountable for ongoing AML/CTF compliance, including supervising internal controls, ensuring the proper escalation of suspicious activity, and serving as the primary point of contact with the FIU Curaçao and the Curaçao Gaming Control Board (GCB).
- **Policies and Procedures:** Operational AML measures, such as Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), transaction monitoring, and reporting protocols, are regularly reviewed and updated to ensure legal alignment and operational effectiveness. The MLRO oversees these measures, and the Operations Team ensures their consistent application.
- **Training and Awareness:** All relevant staff, including third-party contractors, receive role-specific AML/CTF training. Refresher training is conducted annually or following regulatory changes.
- **Monitoring and Reporting:** Both automated and manual systems are employed to identify unusual transactions. Any such activity is escalated to the MLRO, who determines the need for a Suspicious Transaction Report (STR) to be filed with FIU Curaçao.
- **Review and Audit:** This Policy and its operational elements are reviewed at least annually. Internal audits may be conducted to assess the effectiveness of the Company's AML framework and reporting obligations.

6. MLRO Identification and Contact

Name:

Contact:

Refer to Appendix D for escalation and reporting details. Changes to the MLRO will be updated in this Policy and reported to relevant authorities.

7. Risk Based Approach

The AMLCFT obliges the Company to adopt and implement a series of measures, policies, controls, and procedures to prevent the financial system or other systems from being abused for PML/FT. To ensure that the PML/CFT measures, policies, controls and procedures adopted are truly effective, the PMLCFT guidance requires the Company to implement the same on a risk-sensitive basis through the adoption of a risk-based approach. The principle behind the RBA is that resources should be directed proportionately in accordance with the extent of the ML/FT risks posed, so that the business, products, and customers posing the highest risks receive the highest attention.

The risk-based approach hinges on two aspects, namely an understanding of the risks one is facing and based on this understanding of risk, the variation of one's controls, policies, measures, and procedures so as to achieve the strongest mitigating effect possible. This calls not only for an assessment of risk that takes into consideration one's business as a whole but also for an assessment of risk that is more focused on individual business relationships or occasional transactions. While the former risk assessment is referred to as the 'business risk assessment', the latter is known as the '**customer risk assessment**'.

8. Business Risk Assessment

The cornerstone of the risk-based approach necessitates that the Company has to carry out and review a business risk assessment of its activities. This assessment will allow the Company to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. Accordingly, the Company has identified the following ML/FT vulnerabilities and risks. Pursuant to the business risk assessment, the Company has drawn up, adopted and implemented this Manual.

In relation to the carrying out, review and updating of the business risk assessment, the Company must be able to monitor and identify changes to its external ML/FT risk environment to respond by adjusting the administration of its services, customers, relationships and delivery methods, etc, in order to mitigate new and emerging ML/FT risks. If and when such changes are identified, the Company's Board of Directors and MLRO will update the business risk assessment, accordingly, maintain a record of such changes, and update systems and controls to manage the said risks.

Specific risk exposure within the Curaçao framework includes increased risks related to non-face-to-face business, certain payment methods, and international customer bases. These are considered in the business risk model, which is reviewed annually or upon material change to Curaçao operations.

9. Risk Management

The Company has identified risks and implemented the following general principles to reasonably mitigate AML exposure, having regard to the source, nature, and scope of the various channels of business, and its target markets:

- The identity of the players is known through appropriate KYC protocols with validation at registration and verification at appropriate thresholds

- It is against the Company's terms and conditions for a customer to have duplicate accounts on one brand and abuse of such is continually monitored.
- All deposits where possible are received from verified sources associated with the player identity.
- restrict payout transactions only to the transaction vehicle used to affect a prior deposit transaction. Where such a closed loop system is not possible, enhanced diligence protocols are activated, including production, review, and retention of identity-verifying documentation.
- Cash transactions are prohibited, either as deposit or payout methods.
- credit is not permitted.
- Intra-account transfers of funds or of tokens, or any redeemable coupon or credit of any kind are not permitted.
- Player activity is actively monitored on a daily basis for suspicious activity; and
- All bets or wager transactions are in electronic format, are recorded and maintained and are auditable.

The AML protocols of the Company are predicated on four "Phases", which, viewed as a complete system, reasonably mitigate any potential AML risk associated with the conduct of the Company's Gaming Operations.

The "Four Phase" risk management	Objective
Phase 1: Identity Validation and Assessment	Validate the account holder.
Phase 2: Source confirmation	Confirm the funds deposited are received from a source verifiably belonging to the account holder
Phase 3: Recurring Conduct Assessment	Continually monitor account activity for potentially suspicious play patterns, behavior or transactions.
Phase 4: Destination Confirmation and Verification	Ensure that pay out transactions are to a destination verifiably belonging to the account holder's identity

Phase 1: Identity Validation and Risk Assessment

The Company shall determine the extent of the application of CDD requirements on a risk-sensitive basis, depending on the ML/FT risks emanating from the customers, products/services, interface, transactions and jurisdictions related to the business relationships it enters into. Use can be made of the flexibility inherent to the risk-based approach in order to better address risk, as the Company can vary the timing and extent of CDD, which is commensurate to the risk profile. The customer risk assessment is to be carried out whenever a customer is registered with the Company and on an ongoing basis.

Captured Data:

- Country
- Full name
- Address
- Email address

- Acceptance of 18+
- Acceptance of Terms and Conditions

The User is required to validate the account by verifying their registered email address prior to accessing the account.

If a customer requests a change to be made to his / her account details the customer would need to submit a request to our customer services team via email with the new information and must also answer security questions associated with the account. All name changes will require validated, documentary proof of change. The following are accepted as forms of verification:

- Marriage Certificate.
- Name Change Certificate; and/or
- Government issued identification

Preliminary screening

Upon creation of a new account, additional checks are also performed, including but not limited to:

- The customer's email/phone number has been registered previously by another customer on any Company-owned or operated website; and
- The customer's details have been registered to any previous account that has been self-excluded

If any of the foregoing screening identifies potential issues, the issues are investigated, and applicable business rules are applied accordingly. Such business rules may result in a variety of potential risk mitigation steps, including closure of the account, escalation for enhanced diligence, limitation of deposit or withdrawal methods, imposition of deposit limits, etc.

If the customer is found to have more than one account open per any one brand, the Fraud Team will take measures to ensure only one account is operational and link any transactions for recording and reporting purposes.

Phase 2: Source Confirmation

To responsibly identify and mitigate the risk that the deposited funds are deposited other than from a source verifiably associated with such account holder information, the company undertakes various checks listed below. The Company notes varying degrees of risk with different payment methods.

The Risk & Fraud team can monitor the following payment method identifiers and use them as an additional means of verifying that the player = the account holder.

Issued To Name - When registering a payment method in the gaming account, the customer is required to enter the name the payment method has been issued to, exactly as it appears on the credit/debit card and/or the bank account. PIQ, the back-office payment management system, automatically undertakes this check each time a new payment method is registered.

Should the name on the payment method not match the name on the customer account, deposits will not be processed.

Debit/Credit cards – The payment gateways will prevent and decline any transactions originating from lost/stolen cards, The Fraud Team would be able to review and request EDD in these instances.

BINs - BINs can be used to verify that a customer's credit card transactions are coming from a particular country. Should a BIN trace to a different country to the customer's residence, an investigation of the account is conducted by Risk & Fraud to determine if there is indeed any risk associated with receiving transactions issued by an end merchant from another country. PIQ has business rules applied that may automatically reject these transactions.

IP Addresses - Should the IP address not match the customer's country, Risk & Fraud receive an automated alert, which may result in a manual review by the Risk & Fraud team, which may include subjecting the customer to EDD, including by contacting the account holder and requesting an explanation. Should the account holder not be aware of the transaction, the Risk and Fraud Team will launch a further investigation. Customers logging in from an IP address of a 'Blocked Country' will be blocked automatically on login, and a pop-up will show inviting the user to contact Customer Support. This would then be relayed to our Risk and Fraud Team for further investigation.

E-Wallets – The Company appreciates the inherently higher risk with users using e-wallets, as these are found to be more attractive to individuals attempting to circumvent due diligence. The Company accepts deposits from popular E-Wallets and has automated checks in place to validate the e-wallet ownership, there is rarely a need for manual checks.

Phase 3: Ongoing Monitoring

More generally, the Company's Payments, Customer Service and Risk & Fraud teams will monitor customers' activities for a number of indicators or signs of suspicious activity. Any indicators will result in a customer's account being flagged and will result in a review by the Risk & Fraud, which may include subjecting the customer to further EDD steps as detailed above. Indicators can include:

- Mismatches in account or payment information.
- Checks against previously investigated customers/accounts.
- Customers who build up large account balances.
- Erratic or unexplained wagering activity.
- Logins from varying locations
- Adding or depositing from multiple payment sources.
- Addition of higher-risk payment methods (e-wallet)
- Large deposits
- Erratic communication

A further, more exhaustive list of indicators can be found in this Policy in **Appendix A**.

If a customer or transaction within the Company's system shows signs of suspicious activity, it is flagged as "high risk". Even if the customer has previously been subjected to EDD, the Risk & Fraud team reviews and records the customer's behavior, recent transactions, account information, payment options, IP addresses used for deposits and transactions, as well as withdrawal activity. If there are signs of suspicious activity, the customer is contacted to request information to complete EDD, and their account is suspended or terminated, depending on the nature of the concern. If the customer is unable to answer the concerns or complete further due diligence, the business

relationship is terminated.

The Company has set appropriate procedures to monitor the customer data, information, and transactions; in this respect, it has set rules and scenarios in its monitoring system to automate the transaction monitoring process, but as a Policy, the Company has set the following:

- i. Keep the customer documentation and data updated – the Company reviews the data and maintains the required documents to make sure they are up to date.
- ii. Execute thorough transaction monitoring to identify unusual transaction behavior, based on data and statistics collected (customer profiling), and gives a different alert according to the risk area identified to the MLRO in order to investigate and decide if suspicious.
- iii. Execution of EDD – the Company has thresholds in line with its risk-based approach of transactions so as to execute EDD, therefore requires valid evidence of Source of Funds (SoF) and other possible evidence for the transaction purpose.
- iv. Assess continuously the controls to be adequate – based on the type of product sold, and the business model it follows, the Company is considering the adequacy of controls imposed and adapts them in case there is anything identified.

Customer Risk Assessment

The Company carries out a Customer Risk Assessment (“**CRA**”) when a User reaches the €2,000 transaction threshold or at any time prior should the users activity trigger alerts or reviews on activity raise suspicion.

As to the extent of the information that the Company collects, it is essential that this reflects the level of ML/FT risk identified through the CRA. Where the risk is medium or lower, a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can suffice. Social media can also be used as a source of information. However, where the risk of ML/FT is higher or licensees have doubts as to the veracity of the information collected, the information obtained would need to be supplemented by means of independent and reliable information and documentation known as Enhanced Due Diligence.

In developing a customer business and risk profile, the Company obtains statistical data to develop behavioral models against which to eventually gauge a customer’s activity rather than collect sources of wealth information such as Official economic indicators such as average national income, average disposable income etc. issued by national public bodies or reputable financial institutions.

Enhanced Due Diligence

The Enhanced Due Diligence (“**EDD**”) is applied whenever the Company identifies any high-risk situations (unusual transactions) and when the player is a PEP (Politically Exposed Person). This entails taking more stringent steps, which may include collecting additional detailed information on the source of wealth and the source of funds, as well as any additional measures deemed necessary to mitigate the risks.

In carrying out the CDD/EDD measures, customers may be allowed to continue using their gaming account while

the Company obtains any necessary information from the customer concerned. However, until the Company obtains the necessary information and documentation from the customer to meet its obligations, the customer is not to be allowed to affect any withdrawals from the account independently of the amount involved.

The MLRO may decide to contact the customer and ask for information on the origin of the source of these funds, known as a Source of Funds request, and request supporting documentation. In the meantime, the withdrawal functionality on the site would be disabled to prevent further withdrawals and encourage verification.

SOF documentation would be received by the Risk and Fraud Team, who would check for validity and check for fraudulent or tampered documents. The MLRO would then review the documentation and decide on the next course of action:

1. Continue the business relationship.
2. Ask for more information/documentation.
3. Terminate the business relationship

Phase 4: Destination Confirmation and Verification

The fourth Phase of the Company's AML/CTF risk mitigation approach is to ensure that payout transactions are to a destination associated with the verified account holder identity. The principal governing payout transaction policy with respect to AML risk management is that payouts will only be processed back into a transaction vehicle from which an initial deposit was made, known as a **closed loop**. Ensuring that deposits originate from a validated individual and similarly ensuring that the payouts to such accounts are issued only to the same validated individual dramatically reduces AML risk for the Company. Deviations from the above-noted policy are only permitted on an exceptional basis and only in the event that the transaction vehicle is precluded or is incapable of receiving the credit transaction.

In such exceptions (i.e. it is impossible to credit back to a previously used deposit vehicle), enhanced diligence is required prior to the processing of such a payout. Account holders will be required to submit verifying documentation to validate their identity, the initial deposit vehicle (credit card, etc.) and the payout destination vehicle. When withdrawing funds, payments of winnings are paid to the account from which deposits have originated, in their correct order. This means that prior to withdrawing to a new deposit method, all previous deposits processed via different payment methods must equal the total amount of withdrawals from the payment.

If a player's deposits via a pre-paid method, then any winnings are to be paid out to a bank account in their name. Prior to payment, players are to provide a bank statement as proof of ownership of the bank account to which they have requested their winnings to be paid out to. Paying out to a bank account greatly reduces the possibility of money laundering as the payment will be subject to bank due diligence checks and we would be paying out to an account registered in their name. Payments to e-wallets, for example would be subject to less checks than a payment made to a bank.

Payments agents have procedures in order to review and check payments, with particular enhanced checks for large transactions to ensure there is no fraud, the transactions make practical sense in the purpose of the business relationship and AML rules are being complied with.

Considerations for processing payment				
Notes	Routing	Withdrawal	Gameplay	AML
• Checking specific payment instructions (payment method/payment schedule) • If KYC for any un-verified payment method(s) has been requested • Previously identified same IP and checking of other linked accounts • if there's any previous concerns or notes from MLRO	• Does customer have a payment option registered • Is Payment method a method through which payments can be processed e.g. prepaid • Is payment method KYC'ed	• Is this the customer's first withdrawal • What is the amount • What is total deposited amount vs total withdrawn amount • Has the customer complained/queried the status of their withdrawals	• Where did the winnings stem from? (Deposit/Bonus/NDB) • Have bonus rules been breached?	• Does gameplay raise suspicion due to bet size / bet pattern? If so, run relevant reports • Has deposit been wagered 1x • Does the customer have a history of wagering deposits 1x • Has the customer been asked to wager his deposit more than 1x in previous communication(s) • Is there deposit stacking?

The Company takes a risk adverse approach, going above suggested guidance from the prescribed risk-based approach, considering the various jurisdictions and payment methods accepted by the Company, the current approach is to request KYC from customers at the first withdrawal stage in line with the CDD guidelines below

10. KYC Process

Customer Due Diligence (CDD)

Player identity verification is mandatory for financial transactions of 2000 Euro or more. Complete Customer Due Diligence (CDD) must be finalized by the time this transaction amount is reached. However, the company enforces basic CDD measures even before this threshold.

Specifically, upon opening an account, the company identifies the customer by gathering essential details such as full name, permanent address, and date of birth. These are the minimum requirements for lower-risk accounts. Additionally, Politically Exposed Person (PEP) status and sanctions screenings are performed at this stage.

The 2000 Euro threshold is calculated daily, including all deposits, withdrawals, and peer-to-peer transfers since the account was created. When a player reaches this threshold, a comprehensive customer risk assessment and any remaining CDD steps must be completed.

The company's player verification process involves two key elements:

- A copy of a valid government-issued photo ID (passport, driver's license, etc.), including both front and back scans.
- A recent utility bill or bank statement (issued within the last three months) confirming the players' name and current address.

While conducting Customer Due Diligence (CDD), the company will allow a customer to keep using their gaming account while gathering the required information. However, specific restrictions apply when the 2,000 Euro transaction threshold is met:

If the threshold is reached due to a deposit, the customer can no longer make additional deposits or withdrawals but can still use the existing funds to play.

If the threshold is reached because the customer wants to withdraw funds, the account will be completely frozen, preventing any further play.

In either case, if the required CDD information and documentation is not received within 30 days of reaching the 2,000 Euro threshold:

The company will terminate the relationship with the player.

Enhanced Due Diligence (EDD)

In higher-risk scenarios stemming from the Customer Risk Assessment, Phase 3 of the risk mitigation strategy prescribes that EDD should be undertaken to attempt to reduce the risk as much as practically possible. The following information and documentation may be requested, relative to the risk level presented:

- Questionnaire on activity
- Statistical data
- Adverse media
- Source of wealth
- Source of funds

The Company takes the approach of soft checks on customers with avoiding contentious touch points for a smooth customer journey and avoiding tipping off the customer to any suspicions. Therefore, requesting the source of funds and wealth documentation is only reserved where the other tools do not reduce the risk to an acceptable level.

Should it be established that a player is considered a risk and other tools do not reduce the risk to an acceptable level, they will be asked to declare their source of income used for their deposits via one of the below accepted forms of proof:

- Salary – Original or copy of a payslip
- Savings – Certified savings certificates
- Sales of Shares – Bank statement clearly showing receipt of funds
- Sales of Property – Signed letter from solicitor/estate agent
- Inheritance – Grant of probate which must include the value of estate
- Insurance – Signed letter from the insurer or other proof
- Gift – Donor's source of income
- Winnings – Other casino winnings being recycled.
-

Thresholds set in Appendix B and the risk-based approach act as trigger points to request and verify the above documentation. PEPs which have been identified and accepted are also required to provide this documentation at an earlier stage than other customers due to the enhanced risk. The purpose of obtaining source of wealth is show the player's declared body of wealth and provide a clearer understanding of whether they can afford to sustain their level of gambling and it corresponds with previously obtained declarations regarding their business purpose. The purpose of obtaining the source of funds is to ensure the funds used to deposit are not proceeds of crime, other for a purpose of financing terrorism or other illicit activity which is being masked and laundered through the Company. In some cases, documentation such as bank statements can be dual-purpose is satisfying the source of funds and source of wealth criteria.

11. Underage Gambling

The legal framework does not allow minors to partake in any gambling activity. It does not allow for any person under eighteen years of age to be registered as a player, and any funds deposited or won by such persons are to be forfeited.

Any players who are proven to have been under the legal gambling age at the time they made any gambling transactions will have the following actions taken on account:

- Accounts to be closed.
- Any winnings and bonuses will be confiscated, and the remaining balance returned (subject to reasonable charges);
- Any winnings that are accrued during such time will be forfeited by the player, and the player is to return to us any such funds that have been withdrawn from their account.
- The payment method will be blocked in PIQ.

If a payment method of a minor is used on an account of a verified adult, the identity of the owner is verified, with

any deposits refunded and winnings voided, and the payment method is blocked. If a customer contacts us to inform us that a minor used their account and payment method to gamble, the above process does not apply, and the customer will be advised of the T&Cs and to contact the relevant authorities.

12. Jurisdiction and Sanction Lists

The Company will assess the level of ML/FT risk emanating from a particular jurisdiction and determine whether a jurisdiction is deemed to be a non-reputable. This section is intended to assist the Company in the application of these obligations in the light of the Financial Action Task Force (FATF). With regards to the type of jurisdiction, the Financial Action Task Force (FATF) identifies 3 categories:

Category 1	Jurisdictions that have strategic AML/CFT deficiencies and to which countermeasures apply.
Category 2	Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not been committed to an action plan developed with the FATF to address such deficiencies.
Category 3	Jurisdictions with strategic AML/CFT deficiencies that have developed an action plan with the FATF and have made a high-level political commitment to address their AML/CFT deficiencies.

All jurisdictions falling within the above 3 Categories are to be considered as posing varying degrees of higher risk of ML/FT. Therefore, the Company is required to include the risks posed by such jurisdiction within its Risk Assessment. Where it is determined that a large business transaction is connected to a jurisdiction falling within one of the 3 Categories, the Company shall conduct enhanced customer due diligence.

The Guidance Note on High-Risk and Non-Cooperative Jurisdictions holds that a connection to a jurisdiction falling within Categories 1, 2 and 3 may take various forms. For instance, a business relationship or a transaction shall be connected to a higher-risk jurisdiction falling within Categories 1, 2 and 3 if the applicant for business, the beneficial owner, the source of funds/wealth or the business/economic activity is situated in or originates from such a jurisdiction and shall therefore be subject to enhanced due diligence.

The Company shall use its discretion in relation to business relationships or transactions connected to the jurisdictions falling within Categories 1, 2 and 3. The Company will also apply the risk-based approach when it comes to the application of EDD measures in this regard. Countries subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations Security Council will also be listed as high-risk jurisdictions. The Company will continue to review available sources for knowledge of deficiencies in combating money laundering and regularly reviews the FATF and Basel AML Index', the Company retains a list of High-Risk jurisdictions and tags registrations from these countries based on IP tracking and applies an inherent higher level of risk to these accounts, resulting in further mitigating measures.

13. Politically Exposed Persons (PEP)

PEP is a person who is or has, at any time in the preceding year, been entrusted with prominent public functions by a state, a community institution (for example, the European Parliament) or an international body (for example, the United Nations), including the following people:

- I. heads of state, heads of government, ministers and deputy or assistant ministers
- II. members of parliament
- III. members of the supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances
- IV. members of courts of auditors or of the boards of central banks
- V. ambassadors, chargés d'affaires, and high-ranking officers in the armed forces
- VI. members of the administrative, management, or supervisory bodies of state-owned enterprises.

The following people are also regarded as PEPs by virtue of their relationship or association with the people listed above:

- I. Immediate family members of the persons listed above, including spouse, partner, children and their spouses or partners, and parents
- II. known close associates of the persons listed above, including persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the PEP with whom they are associated.

PEP status itself does not incriminate individuals or entities. It does, however, put a customer into a higher risk category. Should it be identified that a player is a PEP via our PEP screening carried out on 1st deposit, a decision is to be taken as to whether to keep their account open or not based on the level of risk the player carries. Should the account remain open, the PEP will be subject to further checks due to the elevated level of risk. To mitigate this, the players in question will be requested to verify their accounts and provide Source of Income documentation (Source of Funds + Source of Wealth). Once the customer has been identified as a PEP, or a family member or known close associate of a PEP, senior management and MLRO approval is required before the business relationship continues and they are permitted to access the gambling services. Further, adequate measures, as appropriate, will be undertaken to establish the source of wealth and source of funds which are involved and ongoing monitoring, with further enhanced due diligence as required.

- All PEP's, their family members and close associates will be subjected to enhanced monitoring by the Payments and Fraud team.
- The MLRO will also maintain a register of all relationships involving PEPs, their family members and close associates, that will be regularly reviewed.

Screening is conducted against global and regional sanction lists, including those applicable under Curaçao law.

14. Record Keeping

The retention of records is not only intended to show that the Company complied with its obligations at law but also to assist the relevant authorities and law enforcement agencies in the prevention, detection, analysis or investigation

of possible ML/FT. The Company has to retain records of any business relationship they enter into and of any transaction they carry out, be it an occasional transaction or a transaction that takes place within the context of a business relationship. These records are to include any documentation and information produced or obtained in complying with their obligations under the PMLCFT guidance. These records are not only intended to show that the Company complied with its obligations at law but are also essential for a Company to effectively discharge certain aspects of its AML/CFT obligations like the carrying out, or revision, of its business risk assessment and the carrying out of ongoing monitoring.

The company is committed in keeping the following records:

- I. CDD documents and other documentation and information, and files appertaining to such documentation and information;
- II. Transaction documentation and information, and other accounts and details in relation to the business transactions, whether international or domestic;
- III. Internal reports made to the MLRO;
- IV. External reports about ML/FT, particularly SARs;
- V. A record of AML/CFT training is provided.
- VI. The AML Manuals; and,
- VII. Records of the actions taken to adopt and implement the risk-based approach

The Company will, at a minimum, retain records for a period of six (6) years.

15. Reporting

Internal reporting:

The Company's employees and 3rd party providers are under a legal obligation to report to the MLRO in respect of information that comes to them within the course of their business:

- where they know, or
- where they suspect, or
- where they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing or is involved in actions that relate to criminal conduct.

This report would not be disclosed to anyone other than the MLRO or another person to whom the employee has a duty to report. The Company does not need to have evidence that money laundering is taking place in order to have suspicion. All employees will be encouraged to seek advice from their manager and/or the MLRO if they have any queries. In accordance with industry guidance, the MLRO, when considering whether there are grounds for knowledge or suspicion, may also require further information to be obtained from the customer if necessary.

The MLRO is responsible for ensuring that all employees are aware of their responsibilities and are familiar with the procedure of reporting suspicious transactions or activities. The employees of the Company and key 3rd party providers are aware that non-compliance with this matter may result in legal action, including criminal action, being taken against them. Employees will be trained in accordance with industry guidance regarding training obligations, and such training will be recorded in their personal training records. Employees are informed of who they should make reports to when they join the company, and information about the roles and responsibilities of the MLRO is set

out in staff induction training and in further training on an ongoing basis.

Internal reporting is normally made by the staff member by sending an email to the MLRO, providing a suspicious transaction report ("STR"). The STR should always be sent electronically. The Report needs to be submitted no later than the next working day in accordance with Appendix D.

External reporting:

Reports of unusual or suspicious transactions for Curaçao operations shall be submitted electronically to the FIU Curaçao using its secure portal. Reporting is required whether or not a transaction is completed and must occur without undue delay once suspicion arises.

Upon receiving notice of an internal STR from an employee, the MLRO will review it and undertake additional enquiries to assess whether the customer's activities are potentially suspicious. The MLRO may also decide to review identification information and the customers' previous transactions or request further information to be obtained. After further evaluation, the MLRO will reach a conclusion of whether he knows, suspects or has reasonable grounds to know or suspect that there may be a linkage to money laundering, terror financing of criminal activity. The MLRO's core functions revolve around reporting and are listed below:

- I. Receiving reports of knowledge or suspicion of ML/FT or that a person may have been, is or may be connected with ML/FT from the Company's employees.
- II. Considering such reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT;
- III. Reporting knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the relevant Authority; and
- IV. Responding promptly to any request for information made by the relevant Authority.

16. Training

The Company ensures that its staff fully understand the policies and procedures, together with their importance and relevance to them as individuals and representatives of the company. Further, the Company ensures that its staff are aware they will be committing criminal offences if they contravene the provisions of the legislation or fail to comply with AML/CFT best practices and gambling-industry specific guidance. Training is undertaken and recorded annually.

17. Compliance and Consequences of Non-Compliance

The Company is fully committed to complying with all applicable anti-money laundering and counter-terrorist financing obligations under Curaçao law. All employees, management, and relevant third parties are expected to adhere strictly to this Policy and associated procedures. Failure to comply with AML/CTF

obligations may expose the Company and its personnel to significant regulatory, legal, and reputational risks. Specifically:

- **Internal Consequences:**

Breaches of this Policy may result in disciplinary action, including suspension, reassignment, or termination of employment or contractual relationships.

- **Legal and Regulatory Exposure:**

Non-compliance may lead to regulatory sanctions, administrative penalties, licence suspension or revocation, and potential criminal liability under the *National Ordinance on the Reporting of Unusual Transactions (NORUT)* and related legislation.

- **Personal Liability:**

Employees and officers who knowingly fail to report suspicious transactions or participate in activities contrary to AML laws may be subject to individual investigation and prosecution.

The Company maintains a zero-tolerance approach to deliberate or negligent AML/CTF breaches. All personnel are required to report concerns promptly and cooperate fully with internal investigations and external regulatory reviews. Compliance is monitored continuously by the MLRO and overseen by senior management.

18. Policy History

Version	Date	Responsible Official	Approving Official	Summary of changes
1.0	12/05/2024			

Next review is due by 31/05/2026.

Appendix A: Measures for the Detection of Money Laundering

Profiles to identify suspicious customers/transactions

The following indicators, inter alia, identify suspicious customers/transactions immediately:

- Player details on registration are incomplete
- Invalid telephone number registered
- Zip code does not match address
- Cannot trace Player on online telephone directories or voters roll etc.

- Invalid details registered
- Chosen language seems suspicious compared to player's name
- Registered countries do not match the IP address
- Bin country of credit card does not match the registered country on the account
- Bin country of cards, registered country and IP address are all different
- No linked accounts to show a history of the player
- Players are transacting in large increments
- Players depositing velocity is too fast
- Player is loading the account with funds before starting to play
- Players are trying various deposit amounts when receiving rejections (irregular increments)
- Player is loading more than 2 credit cards on the account
- Name mismatch cards registered on the account
- Links via credit card or wallet are in a different name than that of the player
- Certain bank rejection reasons such as insufficient funds, retain card etc.
- Multiple accounts registered
- Account registered but only activated after a few days
- Playing patterns are erratic and aggressive i.e. large bets placed on single hand/spin

Appendix B: Live alert triggers

The Company has various capabilities for live alert triggers in line with its Control System. Risk and Fraud takes ownership of acting on these set triggers and conducts a risk analysis before deciding what action is required to address the Company's concerns.

Customer Due Diligence (CDD) is an ongoing process, and certain events, behavioral patterns, or customers that hold an inherent risk will be subject to Enhanced Due Diligence or further monitoring measures. The triggers are fully customizable, and it's intended that these triggers will be regularly reviewed for their effectiveness:

TriggerName	Velocity/threshold for trigger
Different_Deposit_Methods	An alert should be triggered when more than (x) deposit methods are used for deposit/deposit attempts within 24 hours.
Substantial_Deposit_Increase	A series of three consecutive successful deposits (located in time) corresponding to the below criteria: First Deposit – X Amount; Second Deposit – Higher than or Equal to (x)*X Amount; Third Deposit – Higher than or Equal to (x)*X Amount. The Third deposit must be at least *** for the trigger to activate

The Company also has set thresholds whereby users' activity and risk will be reviewed with a holistic review. At some thresholds, documentation will be requested to allow further deposits/withdrawals. I.e, KYC, SOF.

Trigger name	Threshold for trigger
Deposit_Over	\$50,000 (Lifetime)
Deposit_Over	\$25,000 (Lifetime)
Deposit_Over	\$10,000 (Lifetime)
Deposit_Over	\$2,000 (Lifetime)

[Type here]

Appendix C: Reporting Suspicious Activity Policy



What is Suspicion?

A person's suspicion normally exhibits the following pattern, moving from left to right along the three boxes. During routine business, an event may happen within your normal customer relationship that triggers a concern. Once concerned, you must take further action, which may include:

- I. Analysis of the customer's account, re-affirming ID verification, and reviewing gaming history.
- II. Discussing concerns with colleagues and managers; and
- III. Making routine follow-up queries to the player in accordance with standard procedures.

Routine enquiries of a customer conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity, is prudent practice. Such inquiries form an integral part of CDD measures and should not give rise to 'tipping off' the player that you have some concerns.

By following this process, you will either return to the 'comfort' state or concerns will remain and/or shift to become 'suspicion'. If you receive what you consider to be a satisfactory explanation of the unusual activity, you can conclude that there are no grounds for suspicion and no further action is required. Having reasonable grounds to suspect is the objective test of suspicion. As soon as you become suspicious, you must report your suspicion, by submitting an STR, to the MLRO and not to your line manager; you must report this no later than the next working day. Identifying money laundering / fraudulent activity is a challenge and employees should never assume that it is not an issue, even with existing customers that you have dealt with for some time. Existing customer relationships pose as great a money laundering/fraud threat as new customer relationships, if not a greater one, as we can become complacent about them. Employees are not expected to play the role of 'detective' or actively search for information that may lead them to suspicion. Instead, during the normal course of your day-to-day activities, the aim is to:

- I. Gain knowledge of the customer;
- II. Remain alert to the possibilities of money laundering.
- III. Consider whether any customer's activity is unusual and potentially suspicious (refer to Appendix A for examples of suspicious activity).
- IV. Report any suspicions by submitting an STR in accordance with this Policy; and
- V. Remember that your suspicions are important to the business.

All employees must report suspicions no later than the following working day by sending an STR to the MLRO, which sets out:

- the subject customer's information;
- The suspicious transaction details;

[Type here]

- The reason for the employee's suspicion

The Company takes a zero-tolerance approach towards money laundering, terrorist financing or any other form of financial crime; The Company will report suspicious activity or suspicious transactions to the relevant authorities in accordance with its licensing obligations and current legislation. Employees must not actively seek out information that will lead to suspicion; Employees must remain alert to the possibilities of money laundering occurring. Where suspicion of activity or transactions has arisen, employees must report it to the MLRO by submitting an STR as soon as possible, whereupon an Internal SAR Form, as set out in the procedures of this policy, will be completed by the MLRO. Then, following any necessary further investigations, the MLRO may submit an SAR to the Supervisory Authority and FSRC. If, following the further investigations, the MLRO decides not to make a report to the domestic Supervisory Authority, the reasons for this will be documented and retained. These records will be kept separately by the MLRO in order that the information not be disclosed accidentally.

Appendix D: Procedure for completing SAR

1. Once the MLRO has received a STR by email from an employee, the MLRO will ensure that an internal SAR is completed in full using the Curacao FIU secure portal.
2. MLRO to ensure that a completed version of the Internal SAR and supporting evidence (including the STR submitted by the employee) has been saved within a personal electronic folder.
3. The MLRO will then send an acknowledgement of receipt to the employee who submitted the STR email.

