

Riotech N.V.

Anti-Money Laundering and Counter-Terrorist Financing Policy

Key Information

Policy Owner	Riotech N.V.
Approver	Boy Hendriks on behalf of statutory Director Ecorpp Management N.V.
Date approved	30 June 2026
Date last reviewed	30 June 2026
Review frequency	Annual
Next review date	June 2027
Responsible for document management	Derek Hendriks, Compliance officer
Security classification	Private and Confidential



- 1. STATEMENT**
- 2. PURPOSE**
- 3. AUDIENCE**
- 4. DEFINITIONS**
- 5. POLICY IMPLEMENTATION**
 - 5.1 Business Risk Assessment**
 - 5.2 Customer Risk Assessment**
 - 5.3 Customer Acceptance Policy**
 - 5.4 Customer Due diligence**
 - 5.5 Ongoing Monitoring**
 - 5.6 Reliance on third parties to perform customer due diligence**
 - 5.7 PEP and Sanctions Screening**
 - 5.8 Reporting of Unusual Transaction**
 - 5.9 Enhanced Due Diligence (EDD) Triggers**
 - 5.10 Anti-Money Laundering Compliance program**
 - 5.11 Internal Policies, Procedures, and Controls**
 - 5.12 Compliance Officer**
 - 5.13 Employee Screening and Training**
 - 5.14 Independent Audit Function**
 - 5.15 Regulatory Examination and Reporting**
 - 5.16 Programme Review and Continuous Improvement**
 - 5.17 Record Retention**
- 6. Compliance and Consequences of Non-Compliance**
- 7. Related Information**
- 8. Contact Information**
- 9. Policy History**



1. STATEMENT

Riotech N.V. (the Company) is dedicated to upholding rigorous standards in its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) approach. Riotech N.V. adheres to all relevant laws and regulations governing AML and CTF, and is devoted to conducting business ethically, transparently, and lawfully, as outlined in this Anti-Money Laundering and Counter-Terrorist Financing Policy (referred to as 'the Policy').

2. PURPOSE

Its purpose is to delineate Riotech N.V.'s:

- Stance on AML and CTF risks; and
- Arrangements for complying with the prevention of money laundering and countering terrorist financing, via the deterrence and detection of those suspected of laundering the proceeds of crime or those involved in the funding or execution of terrorism, and the disclosure to competent authorities.

Set out below are the principles and standards that Riotech N.V. adopts to ensure that money laundering risks identified are appropriately mitigated.

The Policy should be reviewed alongside the pertinent procedures applicable to your role. If you are unsure about the appropriate course of action, unable to adhere to the Policy, or require clarification on any aspect, it is imperative that you promptly consult the Compliance Officer. Failure to comply with the Policy (and associated procedures) due to ignorance or misunderstanding will not be considered an acceptable justification.

Failure to comply with the Policy could bring financial and reputational damage to the Company, including regulatory censure, fines and enforcement action. It could also result in disciplinary action.

3. AUDIENCE

The Policy extends to all personnel affiliated with Riotech N.V., including employees, agency workers, temporary and fixed-term staff, interns, and external third parties engaged by or on behalf of the Company.

4. DEFINITIONS

AML	Anti-money laundering
CTF	Counter-terrorist financing



CDD	Customer Due Diligence – verification measures applied to customers based on their risk rating
EDD	Enhanced Due Diligence – heightened verification measures applied to medium and high-risk customers
UTR	Unusual Transaction Report – the primary reporting mechanism under Curaçao law by which unusual or suspicious activity is reported to the FIU Curaçao. Also referred to as a Suspicious Activity Report (SAR) in some international contexts; however, Curaçao's National Ordinance on the Reporting of Unusual Transactions (NORUT) uses the term UTR.
FIU	Financial Intelligence Unit Curaçao – the unit in Curaçao responsible for the collection, collation, processing, analysis and dissemination of information to combat money laundering and the funding of terrorism
Customer relationship	The commercial relationship between a remote gaming operator and a customer, which is expected to have an element of duration
Money laundering	The process by which criminal or 'dirty' money is legitimized or made 'clean', including any action taken to conceal, arrange, use, or possess the proceeds of any criminal conduct
Operator	A company that holds an operating licence issued by the Curaçao Gaming Authority (CGA)
PEP	Politically Exposed Person – a natural person who is or has been entrusted with a prominent public function, or an immediate family member or known close associate of such a person
Proceeds of crime	Property from which a person benefits directly or indirectly, by being party to criminal activity
Source of funds	Where the funds, money, or cash to finance the transaction come from
Source of wealth	The origins of a person's overall body of wealth (i.e. their total assets), indicating the volume and acquisition of wealth
Terrorist financing	The raising and processing of funds to supply terrorists with resources, through exploitation of vulnerabilities in financial systems
goAML	The web-based reporting platform operated by FIU Curaçao for submission of Unusual Transaction Reports (UTRs)
NORUT	National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)

5. POLICY IMPLEMENTATION

Riotech N.V. combats money laundering and terrorist financing as part of an overall strategy to tackle financial crime, as crimes such as fraud, tax evasion, bribery and corruption and sanctions breaches are predicate offences that precede the act of money laundering.

As part of this, Riotech N.V.:

- Has designated a Compliance Officer, who has the authority to act independently in carrying out their responsibilities;
- Assesses and identifies the risks inherent in its business model and customer relationships;
- Has in place controls to mitigate the risks identified (for example, by conducting Enhanced Due Diligence on customers that represent a higher risk to the company and regularly analysing transactional patterns to identify anomalous behaviours potentially indicative of financial crime); and
- Has in place mechanisms to escalate unusual patterns, suspicious behaviours or other activities that it believes are indicative of financial crime. Specifically, Riotech N.V. is obligated to submit an Unusual Transaction Report (UTR) for any unusual or suspicious activity to the Financial Intelligence Unit Curaçao (FIU) via the goAML portal. Riotech N.V. is registered with the FIU Curaçao and is authorised to submit UTRs through the goAML system at <https://portal.fiucuracao.cw>.

5.1 Business Risk Assessment

This Business Risk Assessment (BRA) is designed to identify, assess, and mitigate risks associated with Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) within Riotech N.V., an online gaming company. This BRA aligns with regulatory requirements and industry best practices to ensure compliance and maintain the integrity of operations.

Operator-Specific Risk Profile

Riotech N.V. operates as an online gaming company licensed by the Curaçao Gaming Authority (CGA). The following operator-specific characteristics inform the BRA:

Products and Services

- Casino games (slots, table games, live dealer)
- Sports betting and esports wagering
- Poker and peer-to-peer gaming
- Promotional bonuses, VIP programmes, and loyalty rewards

Target Markets and Geographic Exposure

- Primary markets: Western Europe, Latin America, parts of Asia-Pacific



- Restricted jurisdictions (where services are not offered): United States, Netherlands, France, United Kingdom, and any jurisdiction designated as high-risk or non-cooperative by FATF, or subject to UN, EU, UK, US, or Australian sanctions
- Customers from higher-risk jurisdictions (e.g. FATF grey-listed or black-listed countries) are subject to EDD

Payment Methods

- Accepted: bank transfer, major credit/debit cards (Visa, Mastercard), e-wallets (e.g. Skrill, Neteller), prepaid cards
- Cryptocurrency: accepted via integrated payment service providers (PSPs); subject to additional transaction monitoring and EDD given the heightened anonymity risk
- PSPs used by Riotech N.V. are subject to minimum contractual due diligence requirements including AML compliance certification and are reviewed periodically

Player Types and Customer Demographics

- Standard retail customers: assessed as low-to-medium risk on onboarding
- High-volume / high-roller players: flagged for EDD and ongoing enhanced monitoring
- VIP customers: subject to a dedicated VIP due diligence protocol, including source of wealth (SOW) verification and senior management approval
- Affiliate-referred customers: affiliates are screened prior to engagement; affiliate channels are monitored for unusual referral patterns

Affiliate and Third-Party Relationships

- Riotech N.V. works with third-party affiliates and PSPs. All affiliates must meet minimum onboarding requirements and are periodically reviewed
- No reliance is placed on third parties for CDD purposes; all CDD is conducted in-house

Risk Identification

Money Laundering (ML) Risks

- High volume and value transactions typical in online gaming present significant ML risk
- The global reach of the platform increases exposure to customers from higher-risk jurisdictions
- Use of cryptocurrencies increases the risk of anonymous fund flows
- VIP and high-roller accounts present elevated risk of layering through large transactions
- Affiliate channels may be exploited by bad actors to bypass controls

Terrorist Financing (TF) Risks

- Operations in or interactions with customers from jurisdictions known for terrorism financing

- Potential for anonymous or pseudonymous transactions to conceal true customer identity

Proliferation Financing (PF) Risks

- Gaming services may be exploited for PF, especially when involving high-risk jurisdictions
- The diverse customer base may include individuals or entities connected to PF activities

Risk Assessment Summary

Risk Category	Likelihood	Impact	Residual Risk Level
Money Laundering (ML)	High – high volume transactions, global reach, crypto exposure	Severe – regulatory fines, reputational damage, licence loss	HIGH
Terrorist Financing (TF)	Medium – higher in regions with known TF activity	Severe – legal implications, regulatory sanctions	MEDIUM-HIGH
Proliferation Financing (PF)	Low to Medium – dependent on engagement with high-risk jurisdictions	High – international sanctions, regulatory compliance	MEDIUM

Mitigation Measures

- Enhanced Due Diligence (EDD) for customers from high-risk jurisdictions, PEPs, high-volume players, and VIPs
- Crypto-specific controls including wallet screening and chain analysis
- Affiliate due diligence and periodic review programme
- VIP-specific due diligence protocol including SOW verification
- Ongoing employee training on ML/TF/PF typologies and regulatory requirements
- Comprehensive record-keeping and timely UTR submission to FIU Curaçao
- Annual or more frequent BRA review by the Compliance Officer and senior management

Risk Appetite

Riotech N.V. establishes a clear risk appetite framework aligned with its strategic goals, regulatory obligations, and ethical standards:

- Low tolerance: non-compliance with AML, CTF, and anti-proliferation financing regulations. Strict measures are in place to prevent and mitigate these risks.

- Medium tolerance: moderate risks associated with new markets or customer segments, provided robust controls and monitoring systems are in place.
- Zero tolerance: engagement in high-risk activities that could significantly impact the company's reputation, legal standing, or financial stability.

The risk appetite is reviewed annually or whenever significant changes occur in the business environment. The Board of Directors and senior management are responsible for ensuring alignment with the evolving risk profile and regulatory requirements.

5.2 Customer Risk Assessment

Riotech N.V. shall conduct a Customer Risk Assessment (CRA) for each player either prior to executing an occasional transaction or at the stage of establishing a business relationship. This assessment must evaluate the specific risks associated with providing services to the customer and form the basis of the customer's risk profile.

CRA Scoring Matrix

The CRA is conducted by reference to the following risk factors. Each factor is scored individually, and the aggregate score determines the customer's initial risk rating:

Risk Factor	Low Risk (Score 1–3)	Medium Risk (Score 4–6)	High Risk (Score 7–10)
Jurisdiction	EEA	Eastern Europe, LATAM, parts of Asia	FATF grey/blacklist, sanctioned states
Transaction Volume	< NAf 2,000 / month	NAf 2,000 – 10,000 / month	> NAf 10,000 / month or irregular spikes
Payment Method	Bank transfer, major card	e-wallet, prepaid card	Crypto, anonymous methods
PEP / Sanctions	No match	Adjacent / family member	Direct PEP or sanctions hit
Adverse Media	None identified	Minor / unsubstantiated	Confirmed criminal / financial crime
Source of Funds	Verified employment / pension	Self-employed, partially verified	Unverified, inconsistent, offshore
Behaviour Profile	Consistent with declared activity	Occasional anomalies	Structuring, rapid in/out, multiple accounts

Risk Rating Thresholds

Aggregate Score	Risk Rating	Due Diligence Level
7 – 21	Low	Standard CDD
22 – 42	Medium	Enhanced Due Diligence (EDD)
43 – 70	High	Enhanced Due Diligence (EDD) with senior management sign-off

Mandatory High-Risk Override

Notwithstanding the aggregate scoring thresholds set out above, the following individual risk factors shall each independently and automatically result in a High risk rating, regardless of the customer's aggregate CRA score: (a) a direct PEP status match or confirmed sanctions list hit; (b) customer residency in or transactions from a FATF grey-listed or black-listed jurisdiction or a jurisdiction subject to UN, EU, UK, US, or Australian targeted financial sanctions; (c) confirmed adverse media linking the customer to money laundering, terrorist financing, or other serious criminal activity; or (d) any other circumstance in which the Compliance Officer determines that a heightened risk rating is required by applicable law or regulation. In such cases, EDD measures and senior management sign-off are mandatory irrespective of the aggregate score.

CRA Review Triggers

The CRA shall be subject to ongoing review and updated where any of the following trigger events occur:

- Change in payment method, particularly to or from cryptocurrency
- Significant increase in deposit or transaction volume
- Expiry of identity documents
- Detection of adverse media or negative news
- PEP status identified or updated
- Sanctions screening match or close match
- Customer behaviour inconsistent with declared source of funds or source of wealth
- Customer designated as a VIP or high-roller
- Gambling harm indicators or responsible gambling interventions
- Any other material change to the customer's profile or circumstances

Periodic Review Frequency

Risk Rating	Level of Due Diligence	Periodic Review Frequency
Low	Customer Due Diligence (CDD)	Annual
Medium	Enhanced Due Diligence (EDD)	Semi-Annual
High	Enhanced Due Diligence (EDD)	Quarterly or more frequently as required

All customers, including those classified as low risk, are subject to an appropriate level of ongoing monitoring. The risk profile of a customer may change during the period of the customer relationship, including where there are responsible gambling risk indicators.

5.3 Customer Acceptance Policy

Please refer to the Customer Acceptance Policy for detailed information regarding Customer Due Diligence, including:

- Due Diligence Framework and Customer Risk Assessments
- Onboarding a New Customer (during the onboarding process as well as at any later stage, Riotech N.V. may request the following documents and information, including but not limited to: first name, last name, email address, username, date of birth, place of birth, country of residence, residential address, identity number, nationality, confirmation that the user is not a PEP, agreement to KYC procedure and that the user is registering to play on their own behalf, acceptance of the Terms and Conditions and Privacy Policy, consent to receive promotional materials (optional), source of wealth / source of funds information)
- Acceptable Verification Documents, which include: unexpired government-issued documents containing photographic evidence (driver's licence, identification card, travel document or passport); residential address documents not older than 3 months (bank statement, utility bill, correspondence from a central or local government authority, a rental or lease agreement)
- Deposit and Withdrawal Methods
- Transaction-Driven Due Diligence
- Reviewing a Customer File
- Dormant Accounts
- Escalation Procedures
- Unusual Transaction Reporting Policy
- Business Risk Assessment
- Supplier Minimum Requirements
- Data Retention
- Safer Gambling Questionnaire
- Source of Funds / Source of Wealth Questionnaire
- EDD Checklist
- Low-Risk Customer Review Checklist
- Medium / High-Risk Customer Review Checklist
- UTR Report Template
- High-Risk Products, Services and Payment Methods



5.4 Customer Due Diligence

In accordance with the AML/CFT/CFP Regulations for Curaçao providers of online gaming (as amended from time to time, with effect from January 2025), the operator is required to undertake Due Diligence measures in the following circumstances:

- When players engage in financial transactions equal to or above NAf 4,000 (approximately EUR 2,000), consistent with the CGA threshold framework;
- When carrying out occasional transactions above the monetary equivalent of NAf 4,000;
- Where there is a suspicion of money laundering or terrorist financing; or
- Where the operator has doubts about the veracity or adequacy of previously obtained customer identification data.

Due Diligence also includes measures aimed at establishing the beneficial owner. If Riotech N.V. has reasonable grounds to believe that the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and must be identified and their identity verified in accordance with EDD procedure.

CDD is the lowest level of due diligence that can be applied and may only be applied where the customer's risk rating is low, both for financial crime and responsible gambling purposes.

CDD must be applied before a customer's account can be opened and before they are able to make a deposit. Where operational processes differ from this standard, the Compliance Officer must be notified and alternative controls documented and approved before implementation, to ensure that any divergence from this standard does not expose Riotech N.V. to regulatory challenge by the Curaçao Gaming Authority.

In order to be considered low risk, the customer must meet all of the following criteria:

- Be an individual aged 18 or over (or 21 or over where applicable). Customers under the legal gambling age are strictly prohibited;
- Be a resident of a country considered low risk;
- Pass automated screening checks performed by SEON Identity Verification Service;
- Provide a valid residence permit (both sides if applicable); and
- Provide a utility bill (less than 3 months old) for gas, electricity, or phone, or a rental invoice. Alternatively, a document from a government department, mortgage statement, or equivalent.
- Have employment status and income levels within the low-risk category.



5.5 Ongoing Monitoring

Riotech N.V. shall conduct ongoing monitoring of all business relationships to ensure that customer activity remains consistent with its knowledge of the customer, including their risk profile and expected behaviour. This includes maintaining accurate and up-to-date identification data, with procedures in place to detect and verify any changes in customer identity.

Riotech N.V. shall periodically refresh identification information, particularly upon key trigger events such as changes in payment methods, document expiry, or uplift to VIP status. The Compliance Officer shall assess whether such changes warrant a reassessment of the customer's risk rating.

In addition, Riotech N.V. shall perform continuous transaction monitoring to identify unusual or inconsistent activity. Where transactions deviate from the customer's known profile or expected patterns, Riotech N.V. shall investigate the reasons for such deviations and, where appropriate, obtain information on the source of funds supporting the transactions. Sufficient documentation must be collected to support this assessment. Based on the findings, Riotech N.V. shall determine whether the activity is suspicious and whether it should be reported to the FIU Curaçao as a UTR.

The extent and frequency of ongoing monitoring shall be applied on a risk-based approach; however, all customers, including those classified as low risk, shall be subject to an appropriate level of ongoing oversight.

5.6 Reliance on Third Parties to Perform Customer Due Diligence

Riotech N.V. conducts all Customer Due Diligence (CDD) internally and does not rely on third parties. All verification of customer identity, address, and risk screening, including sanctions and PEP checks, is performed in-house according to established policies and procedures. Records of CDD are maintained internally, and the operator remains fully responsible for ensuring compliance with all applicable regulatory requirements.

5.7 PEP and Sanctions Screening

Riotech N.V. operates a robust PEP and sanctions screening programme. The following procedures apply:

Sanctions Lists Screened

All customers are screened against the following sanctions lists at onboarding and on an ongoing basis:

- UN Security Council Consolidated List
- EU Consolidated List of Financial Sanctions



- UK HM Treasury / OFSI Consolidated List
- US OFAC SDN and Consolidated Sanctions Lists
- Australian DFAT Consolidated Sanctions List
- Any additional lists as required by the CGA or applicable regulations

Screening Timing and Frequency

- All new customers are screened prior to account opening and prior to the first deposit being accepted
- Existing customers are rescreened at each periodic review, and in real-time or near-real-time when triggered by a list update or a change in customer circumstances
- Screening is conducted via SEON Identity Verification Service, supplemented by manual review where required

PEP Identification

All new customers are required to self-declare PEP status as part of the onboarding process. Automated screening supplements this declaration. Where a customer is identified as a PEP or a family member or known close associate of a PEP, the following applies:

- The customer is automatically escalated to high risk
- EDD measures must be applied prior to or at the point of onboarding
- Source of wealth and source of funds must be verified
- Senior management approval is required before a business relationship is established or continued with a PEP
- Ongoing monitoring is enhanced for all PEP relationships

Match Handling and False Positive Process

- Where a potential match is identified by automated screening, the case is automatically escalated to the Compliance Officer for manual review
- The Compliance Officer shall assess the match against all available information within 24 hours of identification
- If the match is determined to be a false positive, this finding shall be documented with supporting rationale and retained on the customer file
- If the match is confirmed, the Compliance Officer shall determine the appropriate action, which may include: account suspension, enhanced monitoring, refusal to proceed, or submission of a UTR to the FIU Curaçao
- Confirmed matches against sanctions lists shall result in immediate account suspension and mandatory UTR submission
- Escalation for confirmed sanctions matches must occur within 24 hours, with UTR submission to the FIU within 48 hours

5.8 Reporting of Unusual Transactions

Riotech N.V. is obligated to submit an Unusual Transaction Report (UTR) to the FIU Curaçao for any unusual or suspicious activity under the National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99). This includes activity that provides reasonable grounds to suspect involvement in ML, TF, or other financial crimes. The submission of UTRs aids in the freezing of assets and supports the investigation of financial crimes.

Riotech N.V. is registered with FIU Curaçao and is authorised to submit UTRs via the goAML portal at <https://portal.fiucuracao.cw>. All UTRs must be submitted in English.

UTR Triggers and Indicators

The following indicators may trigger internal reporting and further investigation:

- Transactions reported to police or judicial authorities as potentially linked to ML or TF
- Intended transactions involving natural or legal persons listed on UN, EU, UK, US, Australian, or other applicable sanctions lists
- Transactions equal to or exceeding NAf 4,000 (approximately EUR 2,000), including: bank transactions; sale of chips or credits; payment of prizes
- Any transaction that suggests possible ML or TF involvement, such as:
 - Establishing multiple betting accounts with deposits below the reporting threshold, followed by rapid withdrawals
 - Regularly depositing or transacting similar amounts in a structured pattern
 - Funding accounts with various payment methods (e.g. credit cards, prepaid cards, cheques, cryptocurrency) followed by payout requests
 - Unexplained income inconsistent with the customer's financial situation or profile
 - Claiming machine credits or payouts without a jackpot
 - Associations with multiple accounts under different names
 - Frequent betting transactions or cash deposits or withdrawals just below reporting thresholds
 - Large or rapid transactions inconsistent with the customer's known profile
 - Crypto transactions involving high-risk wallet addresses or mixing services
 - Adverse media linking a customer to criminal activity or financial crime investigations

Reporting Procedures

- Internal Reporting: Employees must report unusual or suspicious activities to the Compliance Officer within 24 hours of identification.
- Upon receipt of an internal report, the Compliance Officer shall conduct an initial triage within 24 hours to determine whether the matter involves a confirmed or probable sanctions match. Where a sanctions match is confirmed, the matter is governed by section 5.7 (immediate account suspension; UTR submission within 48 hours). For all other unusual transaction reports, the Compliance Officer shall complete relevant research and due diligence within 5 working days of receiving the



internal report, and in any event prior to the expiry of the 48-hour external reporting window measured from the point at which a reasonable presumption of ML or TF is established.

- External Reporting: If the Compliance Officer determines that the transaction presents a reasonable presumption of ML or TF, they must report it to the FIU Curaçao within 48 hours.
- Submission Method: UTRs must be submitted via the goAML portal at <https://portal.fiucuracao.cw> in English.

5.9 Enhanced Due Diligence (EDD) Triggers

EDD shall be applied, as a minimum, in the following circumstances:

- Customer is classified as medium or high risk based on the CRA scoring matrix
- Customer is identified as a PEP, or a family member or known close associate of a PEP
- Customer is resident in or transacts from a high-risk or sanctioned jurisdiction
- Customer uses cryptocurrency as a payment method
- Adverse media linking the customer to financial crime, corruption, or other criminal activity
- Large or rapid transactions inconsistent with the customer's declared income or profile
- Customer operates or is associated with multiple accounts
- Unusual or unexplained deposit or withdrawal patterns, including structuring below thresholds
- Customer is designated as a VIP or high-roller
- Source of funds or source of wealth is unclear, inconsistent, or cannot be verified
- Third-country business relationships involving unusual correspondent arrangements
- Any other circumstances where the Compliance Officer determines that a heightened level of scrutiny is warranted

EDD shall include, at minimum: additional identity verification, source of funds verification, source of wealth verification, and senior management approval for high-risk customers and PEPs. EDD is subject to the same ongoing review and monitoring requirements as CDD, with enhanced frequency.

5.10 Anti-Money Laundering Compliance Programme

Riotech N.V. is committed to maintaining a robust AML Compliance Programme designed to prevent, detect, and report money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction. The primary objective of this programme is to ensure full compliance with all applicable laws and regulations in Curaçao while safeguarding the integrity and reputation of the company.



The AML Compliance Programme is risk-based and tailored to identify, assess, and mitigate the risks associated with the company's operations, customers, and services. The programme establishes minimum standards and is supported by internal policies, procedures, and controls. It is approved by senior management and is subject to ongoing review and enhancement.

5.11 Internal Policies, Procedures, and Controls

Riotech N.V. shall establish and maintain comprehensive written policies, procedures, and internal controls to combat money laundering, terrorist financing, and proliferation financing. These policies shall:

- Reflect Riotech N.V.'s commitment to compliance with applicable AML/CTF/CFP laws and regulations
- Address customer due diligence (CDD), transaction monitoring, reporting of unusual transactions, and record-keeping requirements
- Provide clear guidance to employees on their responsibilities

Riotech N.V. implements mechanisms to ensure that policies and procedures remain up to date with regulatory developments.

5.12 Compliance Officer

Riotech N.V. appoints a qualified Compliance Officer who is independent from gaming operations. The Compliance Officer shall have sufficient authority, resources, and access to all relevant information necessary to perform their duties effectively.

The Compliance Officer's responsibilities include, but are not limited to:

- Developing, implementing, and maintaining the AML Compliance Programme
- Ensuring adherence to applicable laws and regulations
- Monitoring compliance with internal policies and procedures
- Reviewing and investigating unusual transactions
- Determining whether transactions should be reported to the relevant authorities as UTRs
- Maintaining records of reported transactions
- Providing AML training to staff
- Keeping the AML programme updated in line with emerging risks and regulatory changes
- Reporting regularly to senior management on AML matters
- Managing PEP and sanctions screening matches and escalation

5.13 Employee Screening and Training



Riotech N.V. shall implement procedures to ensure high standards of integrity in hiring practices, including appropriate background checks on employees. All staff receive training on Riotech N.V.'s policies and procedures, including in relation to financial crime. Satisfactory completion of all training is a mandatory requirement and failure to complete or attend training may result in disciplinary action.

Riotech N.V. shall establish an ongoing AML training programme tailored to the roles and responsibilities of employees. Training shall ensure that employees:

- Understand money laundering and terrorist financing risks
- Are aware of applicable laws, regulations, and internal policies
- Can identify and report unusual or suspicious transactions

Training shall be provided to all relevant staff upon hiring and on a periodic basis thereafter. Riotech N.V. shall maintain detailed records of all training activities, including attendance, content, and assessment results, for a minimum of five years.

5.14 Independent Audit Function

Riotech N.V. does not maintain an internal audit function. Compliance with AML and CTF provisions is reviewed by an independent external auditor. The independent audit shall be conducted at least annually, or more frequently if material regulatory changes, significant business changes, or internal findings warrant an earlier review. The responsible party for commissioning the independent audit is the Board of Directors, acting through the Compliance Officer.

The independent audit shall include at least:

- An evaluation of the company's AML, CTF, and counter-financing of proliferation policies and procedures
- Customer file review
- Compliance management assessment
- Transaction testing
- Assessment of training adequacy
- Assessment of compliance with applicable laws and regulations
- Evaluation of the system's ability to identify unusual activity
- Interviews with employees who handle transactions and their supervisors
- A sampling of unusual transactions on and beyond the applicable threshold(s), followed by a review of compliance with internal and external policies and reporting requirements
- An assessment of the adequacy of the record retention system

The audit shall be conducted by qualified personnel who are independent of the AML compliance function. Audit findings shall be documented and reported to senior



management, with recommendations for corrective actions. Riotech N.V. shall ensure timely remediation of any identified deficiencies.

5.15 Regulatory Examination and Reporting

Riotech N.V. shall fully cooperate with the Curaçao Gaming Authority and other relevant authorities by providing timely access to all requested documentation related to its AML Compliance Programme. Riotech N.V. shall maintain and make available, upon request:

- The AML Compliance Programme and related policies
- Risk assessments
- Records of unusual and reported transactions
- Training records
- Audit reports
- Customer due diligence documentation

5.16 Programme Review and Continuous Improvement

Riotech N.V. shall regularly review and update its AML Compliance Programme to ensure its effectiveness in addressing evolving risks. Adjustments shall be made based on internal findings, audit results, regulatory changes, and emerging money laundering and terrorist financing trends.

Senior management shall ensure that the AML Compliance Programme remains effective, adequately resourced, and aligned with Riotech N.V.'s risk profile.

5.17 Record Retention

Riotech N.V. shall maintain comprehensive records in accordance with applicable regulatory requirements. All records shall be retained for a minimum of five (5) years from the date of the relevant transaction, activity, or relationship ending, whichever is the later. The following minimum retention periods apply:

Record Type	Minimum Retention Period
Customer Due Diligence (CDD) records	5 years from end of business relationship
Transaction records (deposits, withdrawals, bets)	5 years from date of transaction
Unusual Transaction Reports (UTRs) and related investigation records	5 years from date of report
Internal investigation and escalation records	5 years from closure of investigation
Employee training records (attendance, content, assessments)	5 years from date of training

Record Type	Minimum Retention Period
Independent audit reports and management responses	5 years from audit completion
Correspondence with regulators and FIU Curaçao	5 years from date of correspondence
PEP and sanctions screening results	5 years from date of screening

Records shall be stored in a secure and accessible manner, capable of being produced promptly upon request by the Curaçao Gaming Authority, FIU Curaçao, or any other competent authority. Following expiry of the minimum retention period, records shall be disposed of securely in accordance with applicable data protection requirements.

6. Compliance and Consequences of Non-Compliance

Violation of this policy may expose Riotech N.V. and its employees to significant risks, including regulatory and legal sanctions, reputational damage, and financial penalties. Employees who fail to comply with the requirements of this policy may face disciplinary actions, up to and including termination of employment.

Non-compliance with applicable anti-money laundering, counter-terrorist financing, or proliferation financing regulations can result in civil or criminal liability for both the company and individuals, including fines, prosecution, and restrictions on operating licences.

Furthermore, violations may undermine the integrity of the company's operations, damage stakeholder trust, and negatively impact business continuity. All personnel are therefore required to adhere strictly to the policy, participate in mandatory training, and promptly report any suspected breaches or suspicious activity.

7. Related Information

Gambling operators that are authorised and regulated in Curaçao must comply with relevant legislation and regulatory requirements including, but not limited to:

- The National Ordinance on Games of Chance (LOK, PB 2024, no. 157)
- AML/CFT/CFP Regulations for Curaçao providers of online gaming (January 2025, as amended)
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
- The National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99)

- Ministerial Decree with general operation of 11 November 2015, laying down the indicators as mentioned in article 10 of NORUT (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2)
- National Decree of 10 July 2015 for the implementation of article 2 of the Sanctions National Ordinance concerning Al-Qaeda, the Taliban, ISIL, ANF and related persons and organisations (N.G. 2015, no. 29)
- National Decree of 10 July 2015 for the implementation of article 2 of the Sanctions National Ordinance concerning Libya (N.G. 2015, no. 28)
- National Decree of 10 July 2015 for the implementation of UNSC Resolutions 1695 (2006), 1718 (2006), 2087 (2013), and 2094 (2013) concerning the Democratic People's Republic of Korea (N.G. 2015, no. 30)
- National Ordinance extension of validity of sanction decrees 2018 (N.G. 2018, no. 34)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)
- European Union Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions
- UK Sanctions List (under the Sanctions and Anti-Money Laundering Act 2018)
- Consolidated List of Financial Sanctions Targets in the UK (HM Treasury – OFSI)
- Consolidated List of all persons and entities subject to targeted financial sanctions under Australian sanctions laws (DFAT)
- United Nations Security Council Consolidated List
- Specially Designated Nationals and Blocked Persons List (SDN List) (OFAC)
- Consolidated Sanctions List (including SSI, FSE, and other non-SDN lists) (US Department of the Treasury – OFAC)

8. Contact Information

For any questions or concerns regarding this policy, or to report suspicious activity, please contact:

Name	Derek Hendriks
Role	Compliance Officer
Email	compliance@ecorpp.com
Escalation	In the event that the Compliance Officer is unavailable or if the matter relates to the conduct of the Compliance Officer, escalate directly to the statutory director via Ecorpp Management N.V.
UTR Submission	goAML portal – https://portal.fiucuracao.cw (English only)
Regulatory Authority	Curaçao Gaming Authority (CGA)



9. Policy History

This document constitutes a reviewed Anti-Money Laundering and Counter-Terrorist Financing Policy and is effective as of 30.06.2026.

