

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	31 Mar 2026
Date last reviewed	31 Mar 2026
Review frequency	Annual
Next review date	Mar 2027
Responsible for document management	Derek Hendriks, Compliance officer
Security classification	Private and Confidential

1. STATEMENT	4
2. PURPOSE	4
3. AUDIENCE	4
4. DEFINITIONS	5
5. POLICY IMPLEMENTATION	6
5.1 Business Risk Assessment	7
5.2 Customer Risk Assessment	10
5.3 Customer Acceptance Policy	11
5.4 Customer Due diligence	12
5.5 Ongoing Monitoring	13
5.6 Reliance on third parties to perform customer due diligence.	13
5.7 Reporting of unusual transactions	13
5.8 Anti-Money Laundering Compliance program	14
Internal Policies, Procedures, and Controls	15
Compliance Officer	15
Employee Screening and Training	16
Independent Audit Function	16
Program Review and Continuous Improvement	17
6. Compliance and Consequences of Non-Compliance	18
7. Related Information	18
8. Contact Information	20
9. Policy History	20

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
Customer relationship	The commercial relationship between a remote gaming operator and a customer, which is expected to have an element of duration.
CTF	Counter terrorist financing
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
FIU	Financial Intelligence Unit Curaçao. This is the unit in Curaçao that is responsible for the collection, collation, processing, analysis and dissemination of information to combat money laundering and the funding of terrorism
Operator	A company that holds an operating license issued by the Curaçao Gaming Authority
PEP	Politically Exposed Person
Proceeds of crime	Property from which a person benefits directly or indirectly, by being party to criminal activity, for example, stolen money, money from drug dealing or property stolen in a burglary or robbery
SAR	A suspicious activity report – the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to the FIU
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 (that is, their total assets), should give an indication of the volume of wealth the person actually has, and how they acquired it.
Terrorist Financing	The raising and processing of funds to supply terrorists with resources, through exploitation of the vulnerabilities in financial systems that allow for an inappropriate level of anonymity and opacity in the execution of financial transactions.

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 offenses that proceed 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 analyzing transactional patterns to identify anomalous behaviors potentially indicative of financial crime); and
- Has in place mechanisms to escalate unusual patterns, suspicious behaviors or other activities that it believes are indicative of financial crime. Specifically, Riotech N.V. is obligated to submit a Suspicious Activity Report (SAR) for any unusual or suspicious activity to the Financial Intelligence Unit Curaçao (FIU). This supports the aims of the law enforcement agencies by allowing the freezing of property where there are reasonable grounds for suspecting that money laundering or terrorist financing may be involved.

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 our operations.

Identification of Risks

Money Laundering (ML) Risks

- Transaction Volume and Value: High volume and value transactions typical in online gaming present significant ML risks.
- Customer Base: The global reach of online gaming platforms increases exposure to customers from high-risk jurisdictions.
- Payment Methods: The use of various payment methods, including cryptocurrencies, increases the risk of ML.

Terrorist Financing (TF) Risks

- Geographic Exposure: Operations in or interactions with customers from jurisdictions known for terrorism financing.
- Anonymous Transactions: The potential for anonymous or pseudonymous transactions can conceal the true identity of customers.

Proliferation Financing (PF) Risks

- Product and Service Offerings: The nature of gaming services may be exploited for PF, especially when involving high-risk jurisdictions.
- Customer Demographics: The diverse customer base may include individuals or entities connected to PF activities.

Risk Assessment

Money Laundering (ML)

- Likelihood: High, due to the nature of the business and the high volume of transactions.
- Impact: Severe, given the potential regulatory fines, reputational damage, and operational disruptions.

Terrorist Financing (TF)

- Likelihood: Medium, with a higher likelihood in regions with known TF activities.
- Impact: Severe, considering the legal implications and potential for regulatory sanctions.

Proliferation Financing (PF)

Likelihood: Low to Medium, dependent on the company's engagement with high-risk jurisdictions.

- Impact: High, particularly concerning regulatory compliance and international sanctions.

Mitigation Measures

Enhanced Due Diligence (EDD)

- Implement EDD procedures for customers from high-risk jurisdictions or with high transaction volumes.
- Conduct regular reviews of customer profiles and transactions to identify unusual or suspicious activities.

Transaction Monitoring

- Employ advanced transaction monitoring systems to detect suspicious activities in real-time.
- Regularly update the monitoring system to incorporate new ML/TF/PF typologies and regulatory changes.

Employee Training and Awareness

- Provide ongoing training for employees on recognizing and reporting ML/TF/PF risks.
- Ensure staff are aware of the latest regulatory requirements and internal policies related to risk management.

Reporting and Record Keeping

- Maintain comprehensive records of all customer interactions, transactions, and due diligence efforts.
- Establish clear procedures for reporting suspicious activities to the relevant authorities in a timely manner.

Regular Risk Assessments

- Conduct regular assessments of the company's risk exposure to ML/TF/PF, adjusting policies and procedures as necessary.
- Engage external experts periodically to review and enhance the BRA framework

Risk Appetite

Riotech N.V. establishes a clear risk appetite framework to determine the level of risk it is willing to accept in its business operations. The risk appetite is aligned with the company's strategic goals, regulatory obligations, and ethical standards.

Tolerance Levels for ML/TF/PF Risks

- **Low-Risk Appetite:** The company has a low tolerance for risks related to non-compliance with anti-money laundering (AML), counter-terrorist financing (CTF), and anti-proliferation financing (APF) regulations. Strict measures are in place to prevent and mitigate these risks.
- **Medium Risk Appetite:** The company may accept moderate risks associated with new markets or customer segments, provided robust controls and monitoring systems are in place.
- **High-Risk Appetite:** The company is unwilling to engage in high-risk activities that could significantly impact its reputation, legal standing, or financial stability.

Aligning Risk Appetite with Business Strategy

The risk appetite is integrated into the decision-making processes across the organization. This ensures that the company's strategic initiatives are pursued within acceptable risk boundaries, particularly concerning ML, TF, and PF.

Risk Appetite Review and Monitoring

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 that the company's risk appetite remains aligned with its evolving risk profile and regulatory requirements.

This Business Risk Assessment underscores the commitment of Riotech N.V. to proactively manage and mitigate risks associated with Money Laundering, Terrorist Financing, and Proliferation Financing. By implementing the outlined mitigation measures, the company aims to safeguard its operations, comply with regulatory obligations, and uphold its reputation in the online gaming industry.

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. The CRA shall be subject to ongoing review and updated where necessary throughout the business relationship, with any changes potentially resulting in an adjusted risk rating. Based on the outcome of the CRA, Riotech N.V. shall apply an appropriate level of Customer Due Diligence (CDD) in accordance with its Customer Acceptance Policy (CAP). The CAP shall define categories of players that present elevated risks of money laundering, terrorist financing, or fraud and provide clear risk indicators for low, medium, and high-risk classifications. It shall also outline the corresponding CDD measures, including ongoing monitoring requirements, and specify the conditions under which services may be refused. In developing and implementing the CAP, Riotech N.V. must ensure full compliance with applicable requirements relating to Politically Exposed Persons (PEPs) and sanctions screening.

The extent of due diligence measures applied will be determined by the customer's risk profile. In doing so, Riotech N.V. has adopted a risk-based approach in accordance with the AML CFT/CFP-Regulations for Curaçao providers of online gaming as of January 9, 2025 (as may be amended from time to time). When determining the risk profile of a customer, consideration is also given to responsible gambling risks.

The following levels of due diligence are applied depending on the final risk rating:

Risk Rating	Level of Due Diligence
Low Risk	Customer Due Diligence
Medium Risk	Enhanced Due Diligence
High Risk	Enhanced Due Diligence

The frequency of periodic reviews and additional heightened monitoring will vary for each risk level.

The risk profile of a customer may change during the period of the customer relationship, for instance, where there are possible gambling harm risks.

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 CustomerCustomer (during the onboarding process as well as anytime later Riotech N.V. can 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 (politically exposed person), agrees to KYC procedure and is registering to play on his/her own behalf, Acceptance of the Terms and Conditions and Privacy Policy, Consent to receive promo mails and offers (optionally), Source of Wealth / Source of Funds information)

Acceptable Verification Documents, which are:

unexpired government-issued document containing photographic evidence:

- Driver's license, 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, department or agency, a rental or lease agreement.

Deposit And Withdrawal Methods

Transaction-Driven Due Diligence

Reviewing A Customer File

Dormant Accounts

Escalation Procedures

Suspicious Activity Reporting Policy

Business Risk Assessment

Suppliers 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

SAR Report

High-Risk Products, Services And Payment Methods

5.4 Customer Due diligence

According to the AML CFT/CFP-Regulations for Curaçao providers of online gaming as of January 9, 2025, the operator has the obligation to undertake Due Diligence measures when:

- When players engage in financial transactions equal to or above 2000 EUR;
- carrying out occasional transactions above the monetary equivalent of 2000 EUR;
- there is a suspicion of money laundering or terrorist financing; or
- the operator has doubts about the veracity or adequacy of previously obtained customer identification data.

Due Diligence also includes measures aimed at establishing 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 undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and we would therefore have to identify them and verify their identity in accordance with EDD procedure.

CDD is the lowest level of due diligence that can be applied and can 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.

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

- Be an individual aged 18+ (or 21+ where applicable). Customers under the legal gambling age are strictly prohibited;
- Be a resident of the countries that are considered low risk;
- Automated screening checks are passed. Such checks are performed by SEON Identity Verification Service;
- A valid residence permit (both sides if applicable); and
- 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 are provided.

- Employment status and income levels are 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 behavior. 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 or document expiry, and 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 any 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 relevant Financial Intelligence Unit (FIU). 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 Reporting of unusual transactions

Riotech N.V. is obligated to submit a Suspicious Activity Report (SAR) to the FIU Curaçao for any unusual or suspicious activity. This includes activity that provides reasonable grounds to suspect involvement in ML, TF, or other financial crimes. The submission of SARs aids in the freezing of assets and supports the investigation of financial crimes.

The following indicators may trigger internal reporting and further investigation:

- Transactions reported to police or judicial authorities as potentially linked to ML/TF.
- Intended transactions involving natural or legal persons listed on UN or EU Sanctions lists.
- Transactions equal to or exceeding EUR 2,500, 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 cash amounts.
 - Funding accounts with various payment methods (e.g., credit cards, prepaid cards, checks, cryptocurrency) followed by payout requests.
- Unexplained income inconsistent with the customer's financial situation or profile.
- Claiming machine credits/payouts without a jackpot.
- Associations with multiple accounts under different names.
- Frequent betting transactions or cash deposits/withdrawals just below reporting thresholds.

Reporting Procedures

- Internal Reporting: Employees must report unusual or suspicious activities to the Compliance Officer within 24 hours of identification.

- **Compliance Officer Review:** The Compliance Officer will conduct relevant research and due diligence within 10 working days of receiving the report.
- **External Reporting:** If the Compliance Officer determines that the transaction presents a reasonable presumption of ML/TF, they must report it to the FIU within 48 hours.
- **Submission Method:** SARs must be submitted via the GoAML portal at <https://portal.fiucuracao.cw> in English.

Training and awareness

All staff receive training on Riotech N.V.'s policies and procedures, this includes training 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.

5.8 Anti-Money Laundering Compliance program

Riotech N.V. is committed to maintaining a robust Anti-Money Laundering (AML) Compliance Program 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 program is to ensure full compliance with all applicable laws and regulations in Curaçao while safeguarding the integrity and reputation of the Casino.

The AML Compliance Program is risk-based and tailored to identify, assess, and mitigate the risks associated with the Casino's operations, customers, and services. The program 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.

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 the Riotech N.V.'s commitment to compliance with applicable AML/CFT/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.

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 Program;
- 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;
- Maintaining records of reported transactions;
- Providing AML training to staff;
- Keeping the AML program updated in line with emerging risks and regulatory changes;
- Reporting regularly to senior management on AML matters.

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, this includes training 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 also establish an ongoing AML training program 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.

Independent Audit Function

Riotech N.V. does not have an internal audit function. Compliance with AML and CTF provisions is reviewed by an independent auditor on a periodic basis.

These tests must include at least:

- An evaluation of the institution's anti-money laundering, counter-terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of 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 with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- 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.

The audit shall assess:

- The adequacy and effectiveness of policies, procedures, and controls;
- Compliance with applicable laws and regulations;
- The effectiveness of transaction monitoring systems;
- The adequacy of employee training programs;
- Record-keeping practices.

Audit findings shall be documented and reported to senior management, with recommendations for corrective actions. The Riotech N.V. shall ensure timely remediation of any identified deficiencies.

Regulatory Examination and Reporting

Riotech N.V. shall fully cooperate with the Gaming Control Board and other relevant authorities by providing timely access to all requested documentation related to its AML Compliance Program.

Riotech N.V. shall maintain and make available, upon request:

- The AML Compliance Program and related policies;

- Risk assessments;
- Records of unusual and reported transactions;
- Training records;
- Audit reports;
- Customer due diligence documentation.

Program Review and Continuous Improvement

Riotech N.V. shall regularly review and update its AML Compliance Program 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 Program remains effective, adequately resourced, and aligned with Riotech N.V.'s risk profile.

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 licenses. Furthermore, violations may undermine the integrity of the casino'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

Customer Acceptance Policy

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

- The National Ordinance on Gambling (LOK, PB 2024, no. 157)
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (January 2025)

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (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 for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity 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 (issued by: Council of the European Union / European External Action Service (EEAS))
- UK Sanctions List (Lists all designated persons, ships, and aircraft subject to sanctions under the Sanctions and Anti-Money Laundering Act 2018)

- Consolidated List of Financial Sanctions Targets in the UK (Includes all entities and individuals subject to financial sanctions in the UK) (issued by: HM Treasury – Office of Financial Sanctions Implementation (OFSI))
- Consolidated List of all persons and entities subject to targeted financial sanctions under Australian sanctions laws (issued by: Department of Foreign Affairs and Trade (DFAT))
- United Nations Security Council Consolidated List (Includes individuals and entities subject to sanctions imposed by the UN Security Council) (issued by: United Nations Security Council Subsidiary Organs Branch)
- Specially Designated Nationals and Blocked Persons List (SDN List) (Primary sanctions list maintained by OFAC)
- Consolidated Sanctions List (includes multiple non-SDN lists such as the Sectoral Sanctions Identifications (SSI) List, Foreign Sanctions Evaders (FSE) List, and more) (issued by: U.S. Department of the Treasury – Office of Foreign Assets Control (OFAC))

These laws and regulations and any additional regulations form the main legal basis for Riotech N.V. to combat money laundering, the financing of terrorism and the proliferation of weapons.

8. Contact Information

For any questions regarding this policy, please contact:

Compliance Department officer. E-mail: compliance.dept@riobet.com.

9. Policy History

This document constitutes a reviewed Anti-Money Laundering and Counter-Terrorist Financing Policy and is effective as of 31.03.2026.