

Riotech N.V.

**Anti-Money Laundering and Counter-
Terrorist Financing Policy**

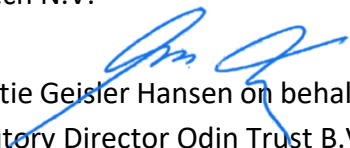
Policy Owner	Riotech N.V.
Approver	 Christie Geisler Hansen on behalf of Statutory Director Odin Trust B.V.
Date approved	31 Mar 2025
Date last reviewed	31 Mar 2025
Review frequency	Annual
Next review date	Mar 2026
Responsible for document management	Maksym Fedorenko, MLRO
Security classification	Private and Confidential

TABLE OF CONTENTS

1. STATEMENT	4
2. SCOPE AND PURPOSE	4
3. LEGAL FRAMEWORK	5
3.1 Rules and regulations	5
3.2 Money laundering	5
3.3 Terrorist Financing	5
3.4 Sanctions	5
3.5 Offences and penalties	6
4. AML & CTF FRAMEWORK	6
4.1 Overview	6
4.2 Customer Due Diligence	7
4.3 Customer Risk Assessment	8
4.6 Training and awareness	8
5. RAISING A SUSPICION	8
5.1 Internal Escalations	8
6. GOVERNANCE	8
6.1 Independent audit	8
6.2 Whistleblowing	8
7. MLRO CONTACT DETAILS	9

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. SCOPE AND PURPOSE

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.

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 Money Laundering Reporting Officer (MLRO). 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. LEGAL FRAMEWORK

3.1 Rules and Regulations

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).

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.

3.2 Money laundering

Money laundering is the process of concealing the origins of money obtained illegally by passing it through a complex sequence of transfers or transactions to turn it into 'clean' money. The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, as well as the legal and regulatory enforcement environment of the market in which the money launderer wishes to operate.

Money Laundering consists of three phases:

1. Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
2. Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
3. Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

3.3 Terrorist Financing

Terrorist financing refers to the provision of funds to support terrorist activities. These funds may originate from various sources, including legitimate ones like personal donations and charities, as well as illicit sources such as drug trafficking, tax evasion, human trafficking, fraud, bribery, and extortion. While there are similarities between the movement of terrorist funds and the laundering of criminal proceeds, pinpointing the exact stage at which lawful

funds transition into terrorist assets can be challenging. Unlike money laundering, where the origin of funds is consistently illicit but their intended purpose can be legal or illegal, in terrorist financing, the source of funds can be lawful or unlawful, but their intended usage is always illicit.

3.4 Financing of proliferation

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

3.5 Sanctions

Sanctions are restrictions on activity with targeted countries, governments, entities, individuals, and industries that are imposed by countries and bodies such as the United Nations or the European Union.

In the context of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) efforts, sanctions can include:

- Financial penalties: Monetary fines imposed on individuals or entities found guilty of AML or CTF violations;
- Legal actions: Criminal or civil proceedings initiated against individuals or entities involved in money laundering or terrorist financing activities;
- Asset freezing and forfeiture: Authorities may freeze assets suspected to be linked to money laundering or terrorist financing, and in some cases, seize or forfeit these assets;
- Regulatory actions: Regulators may revoke licences, suspend operations, or impose restrictions on businesses found to be non-compliant with AML and CTF regulations;
- Reputation damage: Non-compliance with AML and CTF regulations can result in reputational harm for individuals or entities involved, leading to loss of trust from clients, partners, and stakeholders.

Sanctions serve as deterrents to prevent illicit financial activities and promote adherence to AML and CTF standards. They also aim to disrupt the flow of funds to criminal or terrorist organizations, thereby enhancing global security and stability.

3.6 Offenses and penalties

You can face personal liability for failures in Anti-Money Laundering and Counter-Terrorist Financing compliance. Penalties may include fines and imprisonment. Offenses encompass:

- Assisting in concealing, disguising, converting, or transferring criminal proceeds;
- Acquiring, using, or possessing criminal proceeds;
- Failing to promptly disclose knowledge or suspicion of money laundering;
- Alerting suspected money launderers about a filed suspicious activity report or providing information likely to hinder an investigation.

Similarly, significant fines can be levied for sanctions breaches.

4. AML & CTF FRAMEWORK

4.1 Overview

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 appointed a MLRO to have overall responsibility for AML and CTF compliance within the Company. The MLRO has 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.

4.2 Customer Due Diligence

Please refer to the **Customer Onboarding and Escalation Procedures 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 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

4.3 Customer Risk Assessment

A customer risk assessment is conducted for all new customer relationships during the onboarding phase and periodically thereafter, or when certain triggers occur. Information gathered through Customer Due Diligence (CDD) informs the customer's risk profile, which directly influences their individual risk assessment. The customer's risk profile determines

various controls, including the necessity for Enhanced Due Diligence (EDD), the frequency of periodic reviews, and the requirement for heightened monitoring.

4.6 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. RAISING A SUSPICION

5.1 Internal Escalations

When in receipt of an SAR, the MLRO will consider whether an external report should be made to the FIU. You will be guided by the MLRO as to the appropriate steps to take, including if the account should be terminated, as, in some instances, terminating an account could result in tipping off. Please be aware it is unlikely you will be informed of the outcome of an investigation, including as to whether or not a SAR has been submitted.

6. GOVERNANCE

6.1 Independent audit

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

Compliance with AML and CTF must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit must be independent, thus performed by people not involved with the organization's AML compliance staff. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. 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.

6.2 Whistleblowing

Breaches of AML and CTF must be reported. No employee will be subject to disciplinary action where a disclosure has been made in good faith.

7. MLRO CONTACT DETAILS

The MLRO at Riotech N.V. is Maksym Fedorenko, MLRO. Email: compliance.dept@riobet.com.