



**CRYPTO POLICY**



POLICY HISTORY

|                        |                                                                                                                                                                                                                                                                                                                                                       |                     |  |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--|
| Subject                | Crypto Policy                                                                                                                                                                                                                                                                                                                                         |                     |  |
| Purpose                | The Crypto Policy establishes the principles followed by Roobet on how to handle crypto and prevent crypto transactions to be linked to money laundering and terrorism financing activities. It also sets the ground principles of Roobet’s governance framework that ensures appropriate measures are put in place to mitigate crypto exposure risk. |                     |  |
| Responsible Department | Risk Department                                                                                                                                                                                                                                                                                                                                       |                     |  |
| Policy Version         | Approval Date                                                                                                                                                                                                                                                                                                                                         | Changes Description |  |
| V1.0                   | 27/01/2021                                                                                                                                                                                                                                                                                                                                            | Creation            |  |
| V1.1                   | 23/01/2022                                                                                                                                                                                                                                                                                                                                            | Annual Review       |  |
| V1.2                   | 06/02/2023                                                                                                                                                                                                                                                                                                                                            | Annual Review       |  |
| V1.3                   | 14/03/2024                                                                                                                                                                                                                                                                                                                                            | Annual Review       |  |
| V1.4                   | 12/03/2025                                                                                                                                                                                                                                                                                                                                            | Annual Review       |  |



---

## 1. INTRODUCTION

---

Raw Entertainment B.V., (hereinafter “Roobet” or “Company”), is a company duly incorporated under the laws of Curaçao with Company number 157205, and registered office at Korporaalweg 10, Curacao, Curaçao, that operates the website [www.roobet.com](http://www.roobet.com) under the license OGL/2024/687/0427 issued by the Government of Curacao.

---

## 2. DEFENITIONS

---

The below terms shall have the meaning stated below:

| TERMS                        | MEANING                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Crypto</b>                | Refers to all crypto currencies available on the website.                                                                                                                                                                                                                                                                                |
| <b>Employees / Staff</b>     | Means all individuals that have an employment relationship with Roobet or are contractors.                                                                                                                                                                                                                                               |
| <b>Executive Committee</b>   | Means the committee composed by the executive board members that manage de day-to-day decisions of the company.                                                                                                                                                                                                                          |
| <b>MLRO</b>                  | Means Money Laundering Reporting Officer                                                                                                                                                                                                                                                                                                 |
| <b>Money laundering (ML)</b> | Is the term used to describe the process or act of disguising or hiding the original ownership of money that has been obtained through criminal acts such as terrorism, corruption, or fraud. Such monies are then moved through legitimate businesses or sources to make it appear 'clean'. There are three stages to money laundering: |



|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <p><b>a) Placement</b> – is the stage in which funds derived from illegal activities enter a financial system from anywhere in the world.</p> <p><b>b) Layering</b> – involves conducting one or more transactions that are designed to disguise the audit trail and make it more difficult to identify the initial source of funds.</p> <p><b>c) Integration</b> – is the stage in which the funds are disbursed back to the money launderer in what appear to be legitimate transactions.</p>                                                                                            |
| <b>Terrorist financing (TF)</b> | <p>Is a term used to describe the financial crime of using funds to support the agenda, activities, or cause of a terrorist organization. The funds can be from criminal sources and/or legitimate sources. The most common methods of terrorist financing include:</p> <ul style="list-style-type: none"><li>• Criminal activities resulting in ransom demands;</li><li>• Private donations;</li><li>• Donations directly or indirectly through charitable organizations;</li><li>• Revenue from legitimate businesses; and</li><li>• Illicit revenue form criminal activities.</li></ul> |
| <b>Website</b>                  | <a href="http://www.roobet.com">www.roobet.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

### 3. PURPOSE

---

The purpose of this policy is to ensure that Roobet complies with the obligations and requirements set out by the applicable regulation namely regarding the prevention, identification and reporting of money laundering and terrorist financing when handling crypto transactions. This includes ensuring that there



is a governance framework in place that sets adequate procedures and controls to mitigate the risks connected with the use of crypto currencies.

This Policy, in conjunction with the AMLTF Governance Framework, is intended to support Roobet in:

- Assessing the risks of the use of crypto currencies;
- Carry out risk assessments and identify areas where there may be a heightened vulnerability to ML and TF;
- Prepare, maintain, and approve written policies, procedures and controls detailing how Roobet manages the risk connected with crypto transactions;
- Provide training and guidance to all employees on how to effectively implement the policies and controls outlined within, and how to monitor the risks and outcomes; and
- Monitor the effectiveness and adequacy of the Company's policies and controls, and make improvements where required.

---

#### 4. APPLICABILITY

---

This Policy applies to all Roobet's Staff and Contractors that work, collaborate or partner with Roobet (meaning permanent, fixed term, and temporary employees, any third-party representatives, contractors or subcontractors, agency workers, volunteers, interns, and agents engaged with Roobet, regardless of level or seniority). The adherence to this Policy is mandatory and the non-compliance with the same can lead to disciplinary action.

---

#### 5. GOVERNANCE & OVERSIGHT

---

Roobet has implemented a governance framework to mitigate crypto risk that encompasses appropriate governance and oversight roles, internal controls, and sound practices for the management and supervision of the risks associated with crypto and that follow the principles set on the Anti-Money Laundering Policy.

- **Executive Committee** – The members of Roobet's Executive Committee are responsible for ensuring that they understand the risks that are linked with use of crypto currencies. They are accountable for approving the Crypto Policy as well as monitoring the effectiveness of the controls set in place to control the crypto risk. The Board is also responsible for receiving periodic reporting from the Risk Department on adherence to the requirements established within this Policy and to provide further direction, if required.
- **Risk Director** – The Risk Director is designated as responsible for implementing the Crypto Policy and processes. The main responsibilities of the Risk Director include:



- To design and implement the crypto program that complies with the principles set in the Anti-Money Laundering Policy;
  - To verify adherence to local laws and regulations regarding crypto currencies;
  - To organize training sessions for the staff on various compliance-related issues;
  - To make necessary changes to the crypto program;
  - To remain informed on the local and international developments on crypto regulation and to make suggestions to management for improvements.
- **MLRO** – Roobet's MLRO has been designated as responsible for the transaction monitoring and prevent AMLFT. The MLRO, just like for Fiat currency is responsible for:
  - Analysing crypto transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
  - Reviewing all internally reported unusual crypto transactions for their completeness and accuracy with other sources;
  - Keeping records of internally and externally reported unusual transactions;
  - Executing closer investigation of unusual crypto transactions and transactions with high risk exposure.

---

## 6. WHAT IS CRYPTOCURRENCY?

---

As defined by Binance, *“a cryptocurrency is a digital currency secured by cryptography. It's a digital asset typically used as a medium of exchange. Cryptocurrencies can operate globally, 24/7, and independently of intermediaries such as banks and payment processors. The decentralized nature of cryptocurrencies facilitates peer-to-peer (P2P) transactions directly between individuals. So, instead of physical wallets and bank accounts, people access their crypto through unique crypto wallets or crypto exchanges.”*

So, in conclusion cryptocurrency is digital decentralized token that allows people to make payments directly through an online system and without the need of using a bank or other payment methods.

---

## 7. ACCEPTED CRYPTO

---

There are multiple types of cryptocurrencies available worldwide. However, some cryptocurrencies due to their natura cannot be classified as secure. In that sense, Roobet only accepts cryptocurrencies that are classified as “Stable Coins” and are recognized by Governments and Crypto Exchanges as secure.



Roobet accepts the following cryptocurrencies on its website:

- Bitcoin (BTC);
- Ethereum (ETH);
- Solana (SOL);
- Tether (USDT);
- USDC;
- BNB Chain (BNB);
- XRP;
- Tron (TRX);
- Litecoin (LTC); and
- Dogecoin (DOGE).

---

## 8. CRYPTO RISK ASSESSMENT

---

The use of crypto is usually connected with 2 major risks, (i) the anonymity of the owner of the funds and (ii) the source of the funds. Accordingly, Roobet has established a crypto risk assessment that is split in 2 (two stages), Customer Risk Assessment and Transaction Monitoring. The implementation of both stages is ensured through the development of internal procedures and the use of external software tools that help identify risky players and prevent them from conducting illicit activities on the website.

### 8.1. Customer Risk Assessment

As mentioned in Roobet's Anti-Money Laundering Policy, all Roobet customers must provide personal information on registration that allows Roobet to mitigate the anonymity risk that is linked to crypto. The implementation of the above procedures is ensured through the use of the following systems:

- **Customer Information Form** – All customers must provide personal information upon registration, namely Full Name, Date of Birth, Permanent Address and Phone. The non provision of such information will not allow the customers to open an account at the website nor deposit any funds. Roobet will collect the customer's personal details to form a reasonable belief that it knows the identity of its customers commensurate with the user's risk profile. The customer must provide the following information upon registration: full name; permanent residential address; date of birth; place of birth; nationality; and identity number.
- **Customer Verification** - All customers will be requested to comply with ID and POA verification and must comply by uploading the requested documents in a timely manner to ensure Roobet Accounts can be used without restrictions.
- **PEP & Sanction Screening** – Roobet utilizes a third party screening service that cross the customers personal information with global sanctions lists to confirm that the customers are not



subject to United States, European Union, or other global sanctions or watch lists, including individuals or entities associated with the United States' comprehensively sanctioned jurisdictions, Iran, Iraq, Afghanistan, Cuba, North Korea, Syria and the Russian occupied regions of Ukraine.

From performing the CDD upon the customer onboarding, Roobet is able to determine the customer risk profile and decide if it needs to apply additional due diligence measures. Depending on the results, of the risk assessment Roobet might apply Enhanced Due Diligence actions on the players.

## 8.2. Crypto Transactions Monitoring

Roobet understands that crypto transactions have multiple risks. So it has set multiple controls and processes that help detect and identify and prevent suspicious crypto transactions. The system is split into 3 parts:

- Crypto transaction limits;
- Crypto transactions checks;
- Ongoing Monitoring.

## 8.3. Crypto Transaction Limits

The Crypto transaction limits are a set of rules that Roobet has implemented into his system and that limit the way players can use crypto on the website:

- **Limited Cryptocurrencies** – Players can only use the cryptocurrencies on the website and that are recognized by authorities and other organizations as stable coins. This limits the opportunities for the players to use suspicious currencies that might be connected with illicit activities.
- **Anti-Mixing** – Player can only deposit and withdraw the same cryptocurrency. This avoids players from trying to use one currency to deposit and another to withdraw, mixing the funds and trying to hide its source.
- **Anti-Exchange** - Roobet does not provide exchange services. Crypto Assets and Fiat Assets cannot be regularly exchanged through the website.
- **Wallet Checks** – Roobet has a list of prohibit wallets, which are wallets that it has identified has belonging to sanction entities, criminals, or other high risks. If a player tries to use any of the addresses on the list, his account will be automatically fully restricted and reported to the authorities.

## 8.4. Crypto Transaction Checks



Roobet monitors all the crypto transactions that happen on its website. To help performing these checks, Roobet has onboarded **Chainalysis**, an AML blockchain platform that collects information regarding crypto transactions and their potential connection to money laundering, terrorism financing or scams.

Chainalysis has 2 main tools that are used to monitor crypto transactions:

- **Reactor** – It is a platform that allows to track the crypto transactions and create clusters that identify the source of the funds;
- **Know Your Transaction (KYT)** – It is a money laundering detection system that triggers alerts regarding transactions that have an exposure to money laundering risk, terrorism financing or scam.

Every crypto transaction that happens on the website (deposits and withdrawals) go through Chainalysis which will analyse the source of the funds on the blockchain and categorize the transaction as:

- **Low Risk**  
The source of the funds is connected to reputable services that perform KYC or are regulated.
- **Medium Risk**  
The source of the funds comes from services that are not regulated and might not perform full KYC but are known and possible to identify.
- **High Risk**  
The source of the funds is potentially connected to “grey/black markets” that are connected to potential illicit activities but that are not connected to criminal or sanctions individuals or organizations.
- **Severe Risk**  
The source of the funds is connected to criminal or sanctions individuals or organizations.

In order to insert each transaction in any of the above risk categories, Chainalysis looks at:

- **The source of the transaction** – Do the funds come directly from a risky source, or are they indirectly exposed to a risky source that is contaminating the wallet or is the wallet an intermediary to try to disguise the funds; and
- **Blockchain Risk** – Are the funds exposed to Money Laundering and Terrorism Financing categories found on the blockchain:

| Category | Description | Risk |
|----------|-------------|------|
|----------|-------------|------|



|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |        |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| <b>ATM</b>                | ATMs facilitate the conversion of physical cash into cryptocurrency, or cryptocurrency into physical cash. They operate similar to normal fiat ATMs and typically have a KYC requirement (with smaller amounts requiring less KYC info and larger amounts requiring more KYC info). The possibility for exploitation is often dependent on the ATM's KYC requirements.                                                                                                                                                                                                                                                                                              | Low    |
| <b>P2P Exchange</b>       | Peer to peer (P2P) exchanges are online sites that facilitate the buying, selling, and trading of cryptocurrency between two individuals while, usually, not being directly in possession of the funds. Some P2P exchanges will not require any KYC.                                                                                                                                                                                                                                                                                                                                                                                                                | Low    |
| <b>High Risk Exchange</b> | We designate an exchange as high risk according to the following criteria: <ul style="list-style-type: none"><li>• <b>No KYC:</b> The exchange requires absolutely no customer information before allowing every level of deposit or withdrawal. Or they require a name, phone number, or email address but make no attempt to verify this information.</li><li>• <b>Criminal ties:</b> The exchange has criminal convictions of the corporate entity in relation to AML/CFT violations.</li><li>• <b>High risky exposure:</b> The exchange has high amounts of exposure to risky services such as darknet markets, other high risk exchanges, or mixing.</li></ul> | Medium |
| <b>Mixing</b>             | Mixers are websites or software used to create a disconnection between a user's deposit and withdrawal. Mixing is done either as a general privacy measure or for covering up the movement of funds obtained from theft, darknet markets, or other illicit sources.                                                                                                                                                                                                                                                                                                                                                                                                 | Medium |
| <b>Ransomware</b>         | Ransomware is special malware designed to encrypt a victim's computer data and automatically request a ransom to be paid in order to decrypt the data. Attackers employ social engineering and phishing schemes that trick people and organizations into downloading the malicious software.                                                                                                                                                                                                                                                                                                                                                                        | Medium |
| <b>Malware</b>            | Malware can be a type of malicious software that is specifically designed to harm or disrupt computer systems, networks, and devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Medium |
| <b>Fraud Shop</b>         | Financially motivated shops selling different types of data including, PII (Personally Identifiable Information), credit card data, stolen accounts,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Medium |



|                                   |                                                                                                                                                                                                                                                                                                            |        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                                   | and more. Unlike darknet markets, fraud shops are normally operated by a single actor/team and are the sole merchant within the service.                                                                                                                                                                   |        |
| <b>Online Pharmacy</b>            | Online pharmacies are online businesses that may engage in the sale and distribution of medications and other substances without proper credentials to operate.                                                                                                                                            | Medium |
| <b>Scam</b>                       | Scams can impersonate a variety of services, including exchanges, mixers, ICOs, and gambling sites. This category also encompasses scam emails, extortion emails, and fake investment services.                                                                                                            | High   |
| <b>Stolen Funds</b>               | Stolen funds comprise instances of hacked exchanges and services. Attackers engage in sophisticated and persistent social engineering, and exploit pre-existing vulnerabilities to transfer funds from exchange hot wallets to their control.                                                              | High   |
| <b>DNM - Darknet Market</b>       | Darknet markets are commercial websites that operate on the dark web, which can be accessed via anonymizing browsers or software such as Tor or I2P. These sites function as black markets by selling or advertising illicit goods and services such as drugs, fraud materials, and weapons, among others. | High   |
| <b>Illicit Actor-Org</b>          | Individuals and/or organizations that operate directly or indirectly in various forms of illicit activities. These entities are directly or indirectly involved with risky entities such as darknet markets, fraud shops, extremist financing, hacking, etc.                                               | High   |
| <b>Protocol Privacy</b>           | Protocol privacy refers to protocols and entities which use privacy features, such as zero-knowledge proofs, to provide privacy features for users.                                                                                                                                                        | High   |
| <b>CAM - Child Abuse Material</b> | Child abuse material includes forums and sites operating on the dark web which facilitate the buying, selling, and the spread of child sexual abuse material.                                                                                                                                              | Severe |
| <b>Sanctioned Entity</b>          | Sanctions refer to entities listed on economic/trade embargo lists, including but not limited to, sanctions lists imposed by the US, EU, or UN, with which anyone subject to those jurisdictions is prohibited from dealing.                                                                               | Severe |
| <b>Terrorist Financing</b>        | Terrorist financing pertains to the funding of designated terrorist groups and affiliates of terrorist groups, entities, and individuals. Financing is                                                                                                                                                     | Severe |



|                         |                                                                                                                                                                                                                                                                                                                                               |        |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                         | fundamental for the survival and operation of terrorist groups and is used to support a multitude of their activities, including recruitment, propaganda, day-to-day activities, and military operations. Terrorist groups and their affiliates secure the flow of funds in a variety of ways, including through the use of cryptocurrencies. |        |
| <b>Special Measures</b> | Special Measures refers to entities or addresses identified by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) as "primary money laundering concern[s]" under its " <a href="#">Section 9714</a> " or <a href="#">USA PATRIOT Act</a> (section 311) authorities.                                          | Severe |

Upon performing the above checks, alerts are generated that identify suspicious transactions and transactions from illicit sources. Roobet reviews each alert and sets controls that will trigger actions such as:

- Automatically reject the transaction due to being exposed to high risk;
- Enhanced Due Diligence;
- Close player account;
- Report to the authorities;

### 8.6. Crypto Ongoing Monitoring

For last Roobet does not only perform a transaction check, it also performs an ongoing monitoring to the player wallets through the Chainalysis KYT tool. Every transactions made by the player is stored in the player register and a risk map of all the transactions done by the player is created to identify the full risk exposure the player has to each risk category.

This allows Roobet to perform a full ongoing monitoring of the player risk and take the adequate actions depending on the player risk at each given moment in time.

---

## 9. INTERNAL TRANSACTIONS

---

Roobet also keeps a track of all of its internal transactions and payments done in cryptocurrency. For that Roobet uses Chainalysis to verify every crypto wallet before sending or receiving funds, to ensure they originate from legit sources and are not being sent to wallets that might be connected with illicit activities.



---

## **10. TRAINING**

---

Roobet has implemented an crypto training program that all new and existing employees that interact with the crypto side of the business need to complete, to ensure they have all the necessary knowledge and skill set to understand crypto risk. The training will be repeated every 3 years or whenever there are changes in the crypto industry that justify such need.

---

## **11. RECORD KEEPING**

---

Roobet maintains records of all checks crypto transactions and checks performed. The record keeping set on this policy follows the record keeping standard set in the Anti-Money Laundering Policy.

---

## **12. APPROVAL & REVIEW**

---

This Policy was reviewed and approved by the Executive Committee of Roobet. This Policy will be reviewed on an annual basis or whenever there are regulatory or internal procedures changes that impact the same. The Risk Director will be responsible for reviewing the Policy and submitted to the Executive Committee approval.