

AML Policy of Lucifer N.V.

Last updated: 16.8.2023

AML (Anti-Money-Laundering) policy of rr.vip

rr.vip is operated by Lucifer N.V. having its office at Zuikertuintjeweg Z/N(ZuikertuinTower), Curaçao.
Company registration number: 162537

Objective of the AML Policy: We seek to offer the highest security to all of our users and customers on rr.vip. For that a three-step account verification is done in order to insure the identity of our customers. The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against fraud and money laundering. We also consider that depending on the residence and origin, the way of payment and for withdrawing different safety measurements must be taken.

rr.vip also puts reasonable measures in place to control and limit ML risk, including dedicating the appropriate means.

rr.vip is committed to high standards of anti-money laundering (AML) according to the EU guidelines and regulations and requires management & employees to enforce these standards in preventing the use of its services for money laundering purposes.

The AML program of rr.vip is designed to be compliant with:

EU : “Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering”

EU : “Regulation 2015/847 on information accompanying transfers of funds”

EU : Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods.

BE : “Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash.

Definition of money laundering.

Money Laundering is understood as:

- The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or of helping any person who is involved in the commission of such an activity to evade the legal consequences of that person's or companies action;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such an activity;

- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Organization of the AML for rr.vip.

In accordance with the AML legislation, rr.vip has appointed the “highest level” for the prevention of ML: The full management of Lucifer N.V. are in charge.

Furthermore, an AMLCO (Anti Money Laundering Compliance Officer) is in charge of the enforcement of the AML policy and procedures within the System.

The AMLCO is placed under the direct responsibility of the general Management.

AML policy changes and implementation requirements. Each major change of rr.vip AML policy is subject to be approval by the general management of Lucifer N.V. and the Anti money laundering compliance officer.

Three step Verification.

1. Step one:

Step one verification must be done by every user and customer to withdraw. Regarding of the choice of payment, the amount of payment, the amount of withdraw, the choice of withdraw and nationality of the user/customer step one verification must be done first. Step one verification is a document that must be filled out by the user/customer himself. Following information's must be filled in: first name, second name, date of birth, country of usual residence, gender and full address.

2. Step two:

Step two verification must be done by every user which makes a deposit over 2000 EUR (two thousand Euro) or withdraws any amount. Until step two verification is done the withdraw, tip or deposit will be hold. Step two verification will lead the user or customer to a subpage where they must send in their ID. The user/customer must take a picture of their ID, while a paperclip with a six-digit random generated number is next to their ID: Only an official ID may be used for ID verification, depending on the country the variety of accepted IDs may be different. There will also be an electronic check if the filled in Data from the step one verification is correct. The electronic check will check via two different data banks to ensure the given information's matches with the filled document and the name from the ID: If the electronic test fails or is not possible the user/customer is required to send in a conformation of their current residence. A certificate of registration by the government or a similar document is required.

3. Step three:

Step three verification must be done by every user which makes a deposit over 5000 EUR (five thousand Euro) or withdraws over 5000 EUR (five thousand Euro) or sends another user over 3000 EUR (three thousand Euro). Until step three verification is done the withdraw, tip or deposit will be hold. For step 3 a user/customer will be asked for a source of wealth.

Customer identification and verification (KYC).

The formal identification of customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC policy.

This identification relies on the following fundamental principles:

A copy of a passport, ID card or driving license, each shown alongside a handwritten note mentioning six random generated numbers. Also, a second picture with the face of the user/customer is required. The user/customer may blur out any information to secure their privacy, besides date of birth, nationality, gender, first name, second name and the picture.

Please note that all four corners of the ID have to be visible in the same image and all details have to be clearly readable. We might ask for all the details if necessary.

An employee may do additional check-up if necessary, based on the situation.

Proof of Address.

Proof of address will be done via two different electronic verifications, with use of two different databases. If an electronic test fails, the user/customer has the option to prove the residence manually.

A recent utility bill sent to the registered address, issued within the last 3 months or an official document made by the government that proves your state of residence will be required. For example: electricity bill, water bill, bank statement or any governmental post addressed to you.

To make the approval process as fast as possible, user/customer has to make sure the document is sent with a clear resolution where all four corners of the document is visible, and the text is readable.

Depending on situation, additional verification might be necessary.

Source of funds.

In case a player wants to deposit over 5000 EUR (five thousand Euro) there is a process of source of wealth (SOW) verification.

Examples of SOW are:

- Business ownership
- Employment
- Inheritance
- Investments
- Family

It is critical that the origin and legitimacy of wealth is clearly understood.

In case any user deposits specified amount (5000 EUR) at once or by multiple transactions their account will be temporarily frozen. An email will be sent to the player asking to pass the SOW verification. The website will show the notification about the verification as well.

rr.vip will also ask for a bank wire/credit card information to further verify the identity of the user/customer. Additional information about the financial situation of the user/customer will be also required.

Verification form for step one.

The verification form will be accessible via the settings page on rr.vip. Every user must fill out the following information:

- First name
- Last name
- Country of Residence
- Gender
- Date of Birth

The document will be saved and processed by an AI. Compliance officer may proceed with additional check-up, if necessary, based on the situation.

Risk management.

In order to deal with the different kinds of risk and different states of wealth in different countries rr.vip will categorize every nation in three different regions of risk.

Region one: Low risk:

For every nation from the region one the three-step verification is done as described earlier.

Region two: Medium risk:

For every nation from the region two the three-step verification will be done at lower amount of deposit, withdraw and tip amounts. Step one will be done as usually. Step two will be done after depositing 1000 EUR (one thousand Euro), withdrawing 1000 EUR (one thousand Euro) or tipping another user/customer 500 EUR (five hundred Euro), Step three will be done after depositing 2500 EUR (two thousand five hundred Euro), withdrawing 2500 EUR (two thousand five hundred Euro) or tipping another user/customer 1000 EUR (one thousand Euro). Also, users from the low risk region that exchange crypto currency to any other currency will be treated like user/customers from a medium risk region.

Region three: High risk:

Players from high-risk regions will be banned. High risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

Additional measurements.

In addition, an AI will look for any unusual activity and report it immediately to a compliance officer of rr.vip.

In addition, a data scientist supported by modern, electronic, analytical systems will look for unusual behaviour like: depositing and withdrawing without betting sessions, attempts to use different bank accounts to Deposit and Withdraw, region changes, currency changes, behaviour and activity changes as well as verifying, if an account is used by its original owner.

Also, a User must use the same method for Withdraw as they used for Deposit, to prevent any Money Laundering.

Enterprise-wide risk assessment.

As part of its risk-based approach, rr.vip has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and determine risks specific to rr.vip and its business. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The Users to

whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of bank's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on rr.vip understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is reassessed yearly.

Ongoing transaction monitoring.

AML-Compliance ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious compared to the customer profile. This transaction monitoring is conducted on two levels:

1) The first Line of Control:

rr.vip works solely with trusted Payment Service Providers which have effective AML policies in place as to prevent the large majority of suspicious deposits onto rr.vip from taking place without proper execution of KYC procedures onto the potential customer.

2) The second Line of Control:

rr.vip makes its network aware so that any contact with the customer or player or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned. These include:

- Requests for the execution of financial transactions on the account;
- Requests in relation to means of payment or services on the account;

Also, the three-step verification with adjusted risk management should provide all necessary information's about all costumers of rr.vip at all time.

Also, all transaction must be overseen by employees who report to the AML compliance officer who report to the general management.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager must also be a subject to due diligence.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behaviour and the transaction counterparty.

These assessments will be done by an automated System, while an AML specialists crosschecks them for additional security.

The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly justifiable).

Any rr.vip staff member must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known of the customer.

3) The third Line of Control:

As a last line of defence against AML rr.vip will do manually checks on all suspicious and higher risk users in order to fully prevent money laundering.

If fraud or Money Laundering has been found the authorities will be informed.

Reporting of Suspicious transactions on rr.vip. During its internal procedures, rr.vip describes in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

Reports of atypical transactions are analysed within the AML team in accordance with the precise methodology fully described in the internal procedures.

Depending on the result of this examination and on the basis of the information gathered, the AML team:

- will decide whether it is necessary or not to send a report to the FIU, in accordance with the legal obligations provided in the Law of 18 September 2017;
- will decide whether it is necessary to terminate the business relations with the customer.

Procedures.

The AML rules, including minimum KYC standards will be translated into operational guidance or procedures that are available on the website rr.vip.

Record keeping.

Records of data obtained for the purpose of identification must be kept for at least ten years after the business relationship has ended.

Records of all transaction data must be kept for at least ten years following the carrying-out of the transactions or the end of the business relationship.

These data will be safely, encrypted and stored offline and online.

Auditing.

Internal audit regularly establishes missions and reports about AML activities. **Data**

Security.

All data given by any user/customer will be stored securely, will not be sold or given to any third party. Only if forced by law, or in order to prevent money laundering data may be shared with the AML-authority of the affected state.

rr.vip will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC)

Contact us:

If you have any questions about our AML and KYC Policy or if you have any complaints about our AML and KYC Policy or about the procedures done with your Account and your Data, please contact us:

- By email: support@rr.vip