Last update: 26.09.2025

AML Policy of XROCKET CORP.

XROCKET CORP. (the "Company") is committed to providing a safe, compliant, and transparent cryptocurrency platform. Our Anti-Money Laundering (AML) Policy describes how we prevent our services from being misused for money laundering, terrorist financing, or other illicit financial activities.

This document gives an overview of the standards of the "Know Your Customer" and Anti-Money Laundering" policies, thereby setting our practices for the prevention of money-laundering activities while dealing with our users.

This Policy applies to all customers, employees, and partners of the Company. By using our services, you agree to the practices described here.

XROCKET CORP. strictly prohibits and actively prevents money laundering and terrorist financing activities by following applicable regulations and implementing international best practices. We are committed to fulfilling the requirements of applicable laws, identity verification mandates, and aiding in the detection of money laundering, terrorist financing, fraud, or any other financial crime.

xRocket is a multifunctional cryptocurrency platform operated by XROCKET CORP., a company registered in Panama. The project provides a user-friendly bot (@xrocket) and platform available at a site (https://xrocket.exchange/) for cryptocurrency management, including: spot trading with market and limit orders supported by trading charts; creation and sending of cryptocurrency checks for distribution; generation of one-time or recurring invoices for instant payments; management of paid subscriptions for Telegram channels and groups with automated access control; secure storage and sending of cryptocurrencies to external wallets or Telegram contacts; and purchasing cryptocurrencies via bank cards or P2P markets. Supported cryptocurrencies include Bitcoin (BTC), Ethereum (ETH), TRON, TON, BNB, USDT, and Solana. The platform emphasizes low fees, secure storage across multiple networks, and integration within Telegram for seamless user experience. It targets a global audience and handles both crypto-to-crypto and fiat-to-crypto transactions through P2P and card purchases. As a virtual asset service provider (VASP), Xrocket must implement robust AML/CTF measures to mitigate risks associated with anonymous Telegram interactions, P2P trading, and high-volume transactions.

While Panama's Law No. 23 of 2015 may not formally apply to XROCKET CORP., the Company voluntarily follows FATF recommendations and relevant international standards to ensure the integrity of its operations.

Prior to accessing xRocket, it is imperative that you read and understand this Policy, as it is among the documents governing the correct and secure use of Services. In case of any uncertainties regarding the contents of this document, it is advised to seek independent professional advice. This Policy delineates the prerequisites for the identification, screening, and continual monitoring of our users and their transactions. Its purpose is to prevent crimes, including money laundering, terrorist financing, sanctions violations, or tax evasion, as well as to ensure the detection of such occurrences and the subsequent reporting thereof. This Policy is an integral part of the Terms of Use.

1. Customer Due Diligence (CDD)

We perform identification and verification of our customers before executing certain transactions or establishing business relationships.

CDD is applied:

- for all customers participating in P2P transactions, regardless of the amount;
- for all customers conducting transactions involving cash settlements or cash exchange flows.
- before any occasional crypto-to-crypto or fiat-to-crypto transaction equal to or exceeding USD 10,000.00 (or equivalent), or when initiating deposits/withdrawals at or above this threshold
- when suspicious activity is suspected regardless of amount
- when there is a reasonable suspicion of ML, TF, or other criminal conduct
- when doubts exist about previously obtained information

The acquisition of information for the purpose of the DD measures enables us to identify:

- Complex or unusually large transactions;
- Unusual transaction patterns lacking apparent economic or visible legitimate purpose;
- Any other activity that, by its nature, may be linked to ML, TF, or other criminal conduct.

In addition, we have the right, after conducting risk-management procedures, to complete DD on a user after establishing a business relationship if:

- It is necessary to avoid disruption to the normal course of business.
- There is no reasonable suspicion of ML or TF.

To fulfill the DD obligations, we reserve the right to:

- Request documents and information concerning a user's activities and the legal origin of funds;
- Request appropriate identity documents to verify a user's identity;
- Request information about a Beneficial Owners of a user;
- Assess the risk profile of a user, select appropriate DD measures, and evaluate the risk of a user's involvement in ML or TF;
- Re-identify a user if doubts arise regarding the accuracy of the information obtained during initial identification;
- Refuse to participate in or carry out any transaction, freeze user’s assets or any transaction if there is suspicion that a transaction is associated with ML or TF, or if a user or another party linked with the transaction is or could be involved in ML or TF.

We collect:

- Government-issued ID (passport or ID card)
- Proof of address (utility bill, bank statement)

- For legal entities: apostilled registration documents and Articles of Association, translated into English
- Information about beneficial owners and source of funds

Customers are assigned a risk profile (low, medium, high). High-risk customers require enhanced due diligence and approval by the AML Officer.

2. Ongoing Monitoring

We continuously monitor transactions and customer activity to detect suspicious patterns.

Monitoring includes real-time and retrospective checks using both internal tools and third-party screening providers.

We pay special attention to:

- Complex or unusually large transactions
- Transactions inconsistent with a customer’s profile
- Cash deposits or withdrawals
- Cryptocurrency flows linked to sanctioned wallets, darknet markets, or high-risk jurisdictions
- Multiple accounts operated from the same IP or showing anonymity-enhancing patterns

3. Sanctions Screening

We screen all customers and beneficial owners against international sanctions lists:

- United Nations
- European Union
- OFAC (U.S. Treasury)

Additionally, we monitor FATF high-risk jurisdictions and apply enhanced controls for customers connected with such countries.

4. Record Keeping

We retain:

- Customer identification documents
- Transaction history
- Communication records
- Other documents provided by the customer

Customer data is stored securely for 5–8 years after the end of the relationship, in accordance with FATF best practices.

5. Employee Training

All employees must understand AML/CTF obligations. XROCKET provides initial and ongoing training, at least annually, covering ML/TF risks, sanctions, and escalation procedures.

6. Customer Responsibilities

Customers must:

- Provide true and accurate information
- Update their data upon request
- Refrain from using the platform for illegal purposes

In inability to perform DD measures we reserve the right to:

- Cease any transaction or business relationship with any user;
- Refuse to perform any transaction or establish business relationship with any user. In failure to perform constant monitoring of a business relationship, we may terminate the business relationship.

7. General

We may update this Policy from time to time in order to reflect, for example, changes to our practices or for other operational, legal or regulatory reasons. You can review the most current version of this Policy at any time available at https://static.xrocket.exchange/aml_policy.pdf. We reserve the right to update, change or replace any part of this Policy by posting updates and/or changes on xRocket. It is your responsibility to 4 check this Policy periodically for changes. Your use of, or access to, xRocket following the posting of any changes constitutes acceptance of those changes.

We reserve the right to modify and amend the list of Restricted Jurisdictions at our sole discretion at any time and from time to time. We reserve the right to deny access to the Services to any person at our sole discretion and without prior notification. We kindly request that you promptly inform us if you fall under the classification of a Restricted Person or if your residence is within any Restricted Jurisdiction. Failure to adhere to this obligation may result in the implementation of DD measures or the termination of your access to xRocket, as deemed necessary by us.

For more information about our practices, DD measures, if you have questions, or if you would like to make a complaint, please contact us by e-mail at support@xrocket.exchange.