

Crypto Risk Management Policy

This policy is addressed directly to **you, the player**, who uses our platform exclusively through cryptocurrency. It aims to help you understand the risks involved and the precautions you must take. While we implement robust protective measures aligned with Curaçao's LOK and best practices, **we do not assume responsibility for your wallet errors, fraudulent activity, or loss due to misuse or negligence.**

1. Crypto-Only Platform

You may deposit and withdraw **only in supported cryptocurrencies** (e.g., BTC, ETH, USDT).

- **Your responsibility:** Use **wallets you control securely**; do not rely on third-party custodial platforms for deposits or withdrawals.

2. Identity Verification and Wallet Screening

All players must complete full **KYC** before being eligible for withdrawals. We screen your wallet address using blockchain analytics to check for ties to mixers, darknet markets, or sanctioned entities.

- **Your responsibility:** Do not use wallets flagged or associated with illicit activity. Doing so may lead to withdrawal delays or account refusal.

3. Source of Funds

High-volume players must submit proof of the origin of funds (e.g., exchange statements, on-chain wallet history, or self-certification).

- **Your responsibility:** Provide documentation if requested truthfully and accurately.

4. Transaction Monitoring

All crypto transactions are monitored in real time. Unusual patterns or large transfers may trigger further review or temporary holds.

- **Your responsibility:** Approve transactions only from your controlled accounts and be prepared to verify any flagged activity.

5. Volatility Risk

To manage market fluctuations, we convert operational balances into stablecoins following treasury protocols with set thresholds.

- **Your responsibility:** Understand that crypto values can change and that stablecoin mechanisms protect liquidity—not guarantee profit.

6. Jurisdiction Compliance

Access from high-risk or sanctioned regions (as defined by FATF and similar frameworks) is blocked. We use geo-IP controls to enforce compliance.

- **Your responsibility:** Ensure you play in approved jurisdictions. Hosting VPN or proxy access that hides your location may violate our terms and trigger restrictions.

7. Ongoing Audit and Review

We conduct regular internal reviews and technical audits of our crypto risk processes, including wallet screening, AML monitoring, and compliance procedures.

- **Your responsibility:** Cooperate fully if we request information for audits or investigations.

8. Security & Fraud Disclaimer

- We implement secure systems, multi-factor authentication (MFA), and blockchain analytics to safeguard your account.
- **However, we do not cover losses resulting from:**
 - Misplaced or leaked private keys
 - Phishing, social engineering, or scams
 - Sharing credentials or wallet access
 - Transaction errors caused by you
 - Unauthorized access via insecure devices or networks
- We also do not provide individual education or training regarding wallet security. This remains **your personal responsibility**.

9. Best Practices for Players

a. Verify the Withdrawal Address:

- Before initiating a withdrawal, carefully verify that the withdrawal address is accurate and belongs to the intended recipient.
- Cross-reference the address with the information provided by the recipient platform or wallet.
- If you are unsure about the address, contact the recipient or the receiving platform for confirmation before proceeding.

b. Ensure Network Compatibility:

- The chosen network for withdrawal must be compatible with the recipient's platform or wallet.
- For instance, if the recipient only supports ERC-20 tokens, you must select the ERC-20 network for your withdrawal.
- Avoid selecting networks based solely on lower transaction fees, as this can lead to your funds being lost if the network is incompatible.

c. Memo/Tag Requirements:

- Some networks require a memo or tag in addition to the address.
- Always check if a memo or tag is required on the withdrawal page and include it if necessary.

- Failure to include a required memo or tag can result in your assets being lost.

d. Minimum Withdrawal Amounts and Fees:

- Check if a minimum withdrawal amount is required and fees for each cryptocurrency.
- These usually can be found on the withdrawal page for each asset.
- Be aware of these and ensure you are sending an amount that meets the minimum requirement.

e. KYC Verification:

- KYC verification is required for withdrawals.
- Make sure you have completed the necessary KYC verification steps before attempting to withdraw.

f. Withdrawal Restrictions:

- There might be temporary withdrawal restrictions in certain situations, such as after a password reset.
- These restrictions are usually lifted automatically after a set period, such as 24 hours.

g. Risk Disclosure:

- Users are solely responsible for their transactions and any losses incurred due to incorrect information or unsupported networks.
- We are not liable for any losses resulting from user errors.