

Cryptocurrency Risk Management Policy

Bullish Entertainment B.V. updated 4th of September 2024

1. Introduction

This policy outlines the procedures and controls for managing the risks associated with using major cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH), Tether (USDT), Litecoin (LTC), USD Coin (USDC), Bitcoin Cash (BCH), Ripple (XRP), Dogecoin (DOGE), and Dai (DAI) as deposit and withdrawal methods on the **Bullsbet.io** platform. These measures ensure compliance with regulations, protect client assets, and maintain operational integrity.

2. Payment Processing

Bullish Entertainment B.V. uses two licensed and regulated payment processors for cryptocurrency transactions:

- **Dream Finance OÜ:** A licensed entity in Estonia, ensuring regulatory compliance with Estonian laws for cryptocurrency transactions.
- **Pay Perform:** A licensed virtual currency service provider regulated in Estonia, Gibraltar, and the United Kingdom.

Both processors handle the secure and compliant processing of deposits and withdrawals, ensuring the highest standards of security and operational integrity. They are also responsible for conducting regular software audits and compliance checks.

3. Client Account Management

- **Unique Accounts:** Each Bullsbet.io client must maintain a unique account tied to specific wallet addresses for all supported cryptocurrencies, including BTC, ETH, USDT, LTC, USDC, BCH, XRP, DOGE, and DAI.
- **KYC Checks:** As part of our Anti-Money Laundering (AML) Policy, clients must complete Know Your Customer (KYC) verification.

4. Deposit and Withdrawal Policy

- **Funding Wallet Consistency:** Clients who deposit funds using any supported cryptocurrency are only allowed to withdraw to the same wallet address from which the deposit originated. This ensures traceability and prevents fraudulent activity.
- **Evidence of Wallet Ownership:** Clients must provide proof of wallet ownership before processing withdrawals. This may include screenshots of the wallet, transaction history, or additional documents requested by the compliance team.

5. Transaction Monitoring and Security

- **Real-Time Monitoring:** All cryptocurrency transactions are continuously monitored for suspicious activities, with alerts generated for irregular patterns.
- **Cold and Hot Wallet Management:** Most client funds are securely stored in cold wallets (offline) by Dream Finance OÜ and Pay Perform. Hot wallets are used for daily transactions and are protected with multiple layers of encryption and security.

6. Custodial Wallet Services and Virtual Asset Services Provided by Partners

Dream Finance OÜ and Pay Perform provide custodial wallet services for all supported cryptocurrencies. Key aspects include:

- **Cold and Hot Wallet Management:** Funds are primarily stored in cold wallets to ensure security, with only operational funds held in hot wallets for day-to-day transactions.
- **Regulatory Compliance and Audits:** Both partners are responsible for regulatory compliance and conducting regular software audits, ensuring adherence to international financial regulations.

7. Regulatory Compliance

Bullsbet.io relies on Dream Finance OÜ and Pay Perform to ensure all cryptocurrency transactions meet the regulatory requirements in their respective jurisdictions. The processors also conduct regular audits of their systems and processes, ensuring secure and compliant handling of virtual assets.

8. Contingency Planning

Bullsbet.io's contingency planning is managed in collaboration with our payment processors. The **Money Laundering Reporting Officer (MLRO)** oversees coordination with partners and handles user communications in case of incidents. Key measures include:

- **Security Breach:** Dream Finance OÜ and Pay Perform will secure funds in case of a security breach, with the MLRO managing the response and user notifications.
- **Regulatory Challenges:** The MLRO will work with legal advisors and partners to address compliance issues and ensure uninterrupted operations.

9. Policy Review and Updates

This policy is reviewed regularly to ensure its effectiveness in managing risks related to cryptocurrency transactions. Updates will be made as needed to reflect regulatory changes, technological advancements, or new emerging threats.