

SPORTTYP.COM

Cryptocurrency Usage Policy

Version Control

Version	Date	Description	Author	Approved By
1.0	November 7, 2025	Document Creation	Compliance Officer	Senior Management 

Contents

Version Control	2
1. Introduction	4
1.1. Purpose	4
1.2. Scope	4
1.3. Legal and Regulatory Framework	4
2. Authorized Cryptocurrency Channels	5
3. Accepted Cryptocurrencies	5
4. Authorized Use and Restrictions	6
4.1. Market and Operational Risk Management	6
5. Deposits and Withdrawals	6
5.1. Wallet Security and Cybersecurity Controls	7
6. AML/CFT Compliance & KYC requirements	7
7. Transaction Monitoring	8
8. Responsible Gaming Controls	9
9. Training and Awareness	9
10. Record-Keeping	9
11. Non-Compliance	10
12. Policy Review	10

1. Introduction

Delphin Blue Ocean B.V. (the “Company” or “Delphin”) is a regulated gambling operator in Curaçao, and is committed to ensuring its operations and its gambling website (website) are not used for money laundering, financing of terrorism, or other illegal activities. Given the fact that the Company accepts cryptocurrencies as a method of payment on its website, it is essential to establish a clear and concise policy governing the use of such digital assets. The Cryptocurrency Usage policy serves as an extension of the Company’s existing Anti-Money Laundering (AML) Policy.

1.1. Purpose

This Cryptocurrency Usage Policy outlines the principles and rules for the use of cryptocurrencies as a payment method on the Company’s website. The objectives of this policy are to:

- Facilitate the safe and transparent use of cryptocurrencies as a payment method;
- Prevent the misuse of cryptocurrencies for money laundering, terrorism financing, or other criminal activities on the Company’s website;
- Ensure strict adherence to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) laws and regulations including Know Your Customer (KYC) principles, as well as all relevant guidelines and regulations issued by the Curaçao Gaming Authority (CGA), so that the Company, its operations, and its website remain fully compliant.

1.2. Scope

This policy applies to:

- All customers(players) who deposit, wager, or withdraw funds using cryptocurrencies on the website;
- All employees and contractors responsible for payment processing, KYC and compliance, and risk management.

1.3. Legal and Regulatory Framework

Delphin operates under the Curacao Licensing regime and adheres to the following:

- National Ordinance on the Reporting of Unusual Transactions (N.G.2017,no.99);
- National Ordinance on Identification of Clients when rendering Services (N.G.2017, no.92);
- Financial Action Task Force (FATF) Recommendations including Recommendation 15 on Virtual Assets and Virtual Asset Service Providers (VASPs);
- European Union Anti-Money Laundering Directives (5th and 6th AMLD) applied as best practice.

The Compliance Officer monitors regulatory developments, ensures this Policy is implemented, and reports quarterly to Senior Management.

2. Authorized Cryptocurrency Channels

Delphin only accepts cryptocurrencies formally available through reliable, (centralized) cryptocurrency exchanges and regulated e-money financial institutions that support cryptocurrencies through the use of e-wallets.

Specifically, the Company works with the following authorized e-money financial institutions:

- Binance Pay
- MiFinity
- SticPay
- Jeton Bank e-Wallet
- Skrill
- WebMoney
- Neteller
- AstroPay

Due diligence is conducted on any crypto exchanges or e-money financial institutions prior to integration with the Company's website. The Company does not engage with unlicensed or high-risk exchanges and wallet providers. Only transfers from licensed financial entities are accepted, and no deposits or withdrawals may be made to or from entities or countries that are blacklisted or subject to sanctions.

3. Accepted Cryptocurrencies

The Company maintains a list of approved cryptocurrencies of over forty-five (45) types of cryptocurrencies in line with the cryptocurrencies available through the thirds party wallet providers, as referred to in paragraph 2, which includes:

- Bitcoin (BTC);
- Ethereum (ETH);
- Litecoin (LTC);
- Tether (USDT).

Any changes to the list of accepted crypto currencies will be subject to the approval of the Company's Compliance Officer or Senior Management.

Cryptocurrencies, such as privacy coins designed to obscure transaction history, are strictly prohibited. Instead, the use of stablecoins is strongly recommended for gambling activities to mitigate the risk of price volatility.

4. Authorized Use and Restrictions

Cryptocurrencies may only be used on the Company's website by players who have successfully registered an account for gambling purposes.

All cryptocurrency transactions by players must be conducted through wallets owned and controlled by the verified account holders.

The Company only accepts cryptocurrencies from players located in jurisdictions where it is authorized to offer its gambling services and products.

Cryptocurrencies may be used solely for the following purposes:

- Deposits into player accounts;
- Wagers placed on the website;
- Withdrawals to a verified (cryptocurrency) wallet owned by the player.

The conversion of cryptocurrencies to fiat currency within the player's account is strictly prohibited. Additionally, Delphin does not offer cryptocurrency investment products or interest-bearing balances on players' account.

4.1. Market and Operational Risk Management

Delphin applies the following measures to mitigate potential market- and operational risks, through the use of Cryptocurrencies:

- Stablecoins (e.g. USDT, USDC) are strongly preferred for significant deposits and withdrawals;
- High-value payouts may be staggered to ensure proper management of liquidity and to apply the appropriate customer due diligence;
- High risk coins(e.g. privacy coins) and mixers are strictly prohibited;
- Regulatory changes are continuously monitored to ensure timely adaptation of the policy and procedures.

5. Deposits and Withdrawals

Players may deposit and withdraw funds from their account using only the cryptocurrencies approved by the Company (*see paragraph 3 'Accepted Cryptocurrencies'*). A player may make deposits into their account using various methods which include e-wallets held with different wallet providers and cryptocurrency exchanges. All available methods and wallet providers are clearly listed on the Company's website and may vary depending on the player's country of residence.

Additionally, the following restrictions apply to all cryptocurrency transactions:

- Deposits and withdrawals are permitted only to and from the same account and via the same payment method used for the original deposit;
- Players may use their deposits solely for gambling purposes; withdrawals will not be permitted without any prior gambling activity on player's account;
- Inter-account transfers between players are strictly prohibited.

5.1. Wallet Security and Cybersecurity Controls

The Company implements the following controls to ensure the safety of digital assets for both cold and hot wallets:

1. Cold wallets

- The Company maintains several cold wallets designated for reserve funds. These wallets are stored in secure location with strictly limited access.
- Access to such wallets requires multiple signature authorization for any transaction to or from the cold wallets. This means that multiple authorized parties must approve a transfer before it can occur, reducing the risk of fraud or unauthorized access.

2. Hot Wallets

- Additionally, the Company maintains several hot wallets for day -to-day transactions including the transactions of players with strict access controls to limit risk exposure.

3. Balance Reconciliation

- Wallets are checked daily against the internal records. Any discrepancies found are immediately investigated and documented by the Payment Processing Team.

4. Access Security

- Access to the Company's wallets (hot and cold) are protected by Multi-Factor Authentication (MFA) to ensure that only authorized staff can gain access and prevent unauthorized use. Access rights of the authorized staff are reviewed regularly.

6. AML/CFT Compliance & KYC requirements

Delphin is required to fully comply with Curaçao AML/CTF laws and regulations. The Company, thus, applies appropriate Customer Due Diligence (CDD) measures to cryptocurrency transactions

in the same manner as to fiat transactions. These measures are designed to prevent its platform from being used for illicit activities including money laundering and the financing of terrorism.

All players, regardless of their chosen payment method, undergo customer due diligence (CDD) in line with the Company's AML policy. Before enabling cryptocurrency deposits or withdrawals, the following steps must, therefore, be completed:

- **Customer identification and verification:**

At the minimum, personal information of the player is collected and verified, which includes full name, date of birth, residential address, and government-issued ID.

- **Verification of ownership of player's wallet:**

The Company verifies that the player controls the (cryptocurrency) wallet used for crypto transactions to prevent fraud and unauthorized use.

- **PEP and Sanctions screening**

Players are screened against global sanctions-and blacklists (e.g., OFAC, UN, EU) to prevent transactions involving sanctioned individuals or entities.

- **Adverse media and PEP screening:**

Players are reviewed for negative news and checked if they are politically exposed persons to determine if enhanced due diligence is needed in accordance with the AML Policy.

7. Transaction Monitoring

The Company applies a risk-based approach to monitor all cryptocurrency transactions for suspicious activity such as:

- Rapid deposit-withdrawal patterns;
- Transactions that are not consistent with the customer's risk profile;
- Structuring transactions to avoid the reporting thresholds;
- Use of privacy-or high risk coins;
- Players having links to sanctioned addresses or mixers.

All transactions are continuously monitored through third-party systems. Bittech uses Sumsb services in order to detect and recognize red flags or suspicious transactions from the players deposits.

All suspicious transactions will be reported to the Financial Intelligence Unit of Curaçao (FIU Curaçao) in accordance with AML/CTF reporting obligations.

8. Responsible Gaming Controls

Delphin is committed to ensuring that players use its gambling platform safely and responsibly. The use of cryptocurrency on the website does not exempt players from the Company's Responsible Gambling Policy. Accordingly, the Company applies the following controls to foster a safe and responsible gambling experience:

- Players are informed immediately of deposit and withdrawal limits for e-wallets upon selecting their payment method;
- Regardless of the choice of their payment method, players can set time limits or self-exclude to manage their gambling activity.

9. Training and Awareness

The Company shall provide all employees with annual training to ensure that they understand the risks, regulatory obligations, and operational procedures related to cryptocurrency transactions.

The training shall cover, at a minimum, the following topics:

- **AML/CFT crypto-specific red flags** – identifying suspicious activities and transaction patterns unique to cryptocurrency;
- **Blockchain analytics** – understanding the use of blockchain monitoring tools for compliance purposes;
- **Cybersecurity best practices** – protecting wallets, credentials, and systems against cyber threats.
- **FATF and Curaçao compliance expectations** – ensuring adherence with both international and local regulatory requirements.

All trainings are carefully documented and records thereof are retained accordingly.

10. Record-Keeping

The Company retains all documents, information and data collected for customer due diligence, ongoing monitoring, transaction monitoring, and players account records for a minimum of five (5) years after the end of the business relationship or the date of the occasional transaction, unless a longer period is required by the relevant authority. All records are kept readily accessible and can be provided to relevant authorities, such as FIU Curaçao and the GCA upon request.

11. Non-Compliance

Failure by employees, contractors, or partners to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and may be reported to relevant authorities. Additionally, non-compliance by players may result in account suspension, closure, and the freezing or forfeiture of funds in accordance with applicable laws and regulations.

12. Policy Review

This Policy will be reviewed annually or prior if there are any changes in the Company's operations, laws or regulations that may impact the content and implementation of the policy. The review and approval will be conducted by the Compliance Officer and senior management.