

Cryptocurrency Usage Risk Policy

Company: Universe B Games B.V.

Legal Form: Limited Liability Company

Registration Number: 155126

Registered Address: Seru Loraweg 17C, Curaçao

Incorporation Date: September 10, 2020

Brand: BetFury

Version: 1.0

Effective Date: 15 June 2026

Policy Owner: MLRO / Compliance Officer

MLRO / Compliance Officer Email: mlro@betfury.com

Approved by: Director, Jevgenijs Curikovs

1. Purpose

This Cryptocurrency Usage Risk Policy sets out Universe B Games B.V.'s approach to identifying, managing, monitoring, and mitigating risks associated with the use of cryptocurrency in its online gaming operations under the BetFury brand.

The Policy is designed to ensure that cryptocurrency deposits, withdrawals, refunds, conversions, and related payment activities are handled in a controlled, transparent, and risk-based manner, in line with applicable AML/CFT, sanctions, fraud prevention, responsible gaming, cybersecurity, and regulatory requirements.

2. Scope

This Policy applies to all cryptocurrency-related activities of the Company, including:

1. Customer deposits and withdrawals using cryptocurrency.
2. Cryptocurrency wallet screening and transaction monitoring.
3. Source of funds and source of wealth checks related to crypto transactions.
4. Use of third-party crypto payment processors, custodians, exchanges, or blockchain analytics providers.
5. Internal controls over crypto payment processing, reconciliation, custody, and reporting.

This Policy should be read together with the Company's AML/CTF Policy, Customer Onboarding and Escalation Procedures, Sanctions Policy, Responsible Gaming Policy, Fraud Prevention Policy, Information Security Policy, Terms and Conditions, and other applicable internal procedures.

3. Governance and Responsibilities

Senior management is responsible for approving the Company's cryptocurrency risk appetite and ensuring that appropriate systems, controls, and resources are in place.

The MLRO / Compliance Officer is responsible for maintaining this Policy, overseeing crypto-related AML/CFT and sanctions controls, reviewing higher-risk activity, escalating suspicious activity, and reporting material issues to senior management.

The Payments, Finance, Risk, Fraud, and Technology teams are responsible for implementing the operational controls required under this Policy.

4. Risk Appetite

The Company recognises that cryptocurrency may present increased risks due to the speed, cross-border nature, pseudonymity, volatility, and potential misuse of crypto-assets.

The Company will only support cryptocurrency payment methods, assets, networks, and providers that can be appropriately monitored, screened, reconciled, and controlled.

The Company will not knowingly accept or process cryptocurrency transactions linked to sanctioned persons, sanctioned jurisdictions, mixers, tumblers, darknet markets, ransomware, fraud, terrorist financing, stolen funds, or other illicit sources.

Where risk cannot be adequately mitigated, the Company may reject, suspend, return, restrict, or escalate the transaction or customer relationship.

5. Supported and Prohibited Crypto-Assets

The Company will maintain an approved list of supported crypto-assets and blockchain networks.

Before supporting any crypto-asset or network, the Company will assess relevant risks, including liquidity, volatility, blockchain analytics coverage, sanctions exposure, illicit finance risk, operational reliability, and the ability to reconcile transactions.

The Company will not support:

1. Privacy coins or assets designed to obscure transaction history, unless specifically approved following enhanced review.
2. Assets or networks that cannot be effectively monitored or screened.
3. Transactions involving mixers, tumblers, darknet markets, ransomware addresses, sanctioned wallets, or other high-risk services.
4. Unapproved tokens, unsupported networks, or crypto products outside the Company's licensed gaming activity.

6. Customer Due Diligence and Transaction Monitoring

Cryptocurrency usage will be considered as part of the customer's overall risk rating.

The Company may apply enhanced due diligence where a customer uses self-hosted wallets, conducts high-value or unusual transactions, uses multiple wallets, shows limited gameplay after deposits, is linked to high-risk jurisdictions, or presents other elevated risk indicators.

Where required, the Company may request source of funds or source of wealth evidence, including exchange statements, proof of crypto purchase, bank statements, trading records, tax records, business income evidence, or blockchain transaction history.

The Company will monitor crypto-related activity on an ongoing basis, including:

1. Rapid deposit and withdrawal activity.
2. High-value deposits with limited or no gameplay.
3. Multiple accounts using the same or linked wallets.
4. Transactions inconsistent with the customer's profile.
5. Activity involving high-risk wallets, chains, jurisdictions, or services.
6. Attempts to bypass KYC, AML/CFT, sanctions, responsible gaming, or withdrawal controls.

Suspicious, unusual, or high-risk activity will be escalated to the MLRO / Compliance Officer for review and further action.

7. Wallet Screening and Sanctions Controls

The Company will apply appropriate wallet screening and blockchain analytics controls to cryptocurrency deposits and withdrawals.

Screening may include checks for exposure to sanctioned wallets, sanctioned persons, darknet markets, mixers, tumblers, scams, ransomware, terrorist financing, stolen funds, fraud, or other illicit sources.

Where a wallet or transaction presents an unacceptable risk, the Company may pause, reject, return, restrict, or escalate the transaction, subject to applicable legal and regulatory requirements.

Potential sanctions matches must be escalated immediately to the MLRO / Compliance Officer and handled in accordance with the Company's Sanctions Policy and AML/CTF procedures.

8. Deposits, Withdrawals, and Customer Disclosures

Cryptocurrency deposits and withdrawals may only be processed through approved payment flows, wallets, providers, assets, and networks.

The Company will clearly inform customers of:

1. Supported crypto-assets and networks.
2. Minimum and maximum transaction limits.
3. Blockchain confirmation requirements.
4. Possible delays caused by compliance checks.
5. Fees, exchange rates, and conversion rules.
6. Treatment of incorrect, unsupported, underpaid, or overpaid transactions.
7. The risks of cryptocurrency volatility and irreversible blockchain transfers.

Withdrawals may be delayed, restricted, or refused where there are unresolved AML/CFT, sanctions, fraud, responsible gaming, cybersecurity, account security, or source of funds concerns.

9. Responsible Gaming, Fraud, and Cybersecurity

The Company will consider cryptocurrency usage within its responsible gaming monitoring framework.

Crypto-related behaviour that may indicate gambling harm includes frequent high-value deposits, escalating deposit patterns, attempts to bypass limits, use of multiple wallets, or activity inconsistent with the customer's known profile.

The Company will also maintain fraud and cybersecurity controls, including monitoring for account takeover, bonus abuse, mule accounts, suspicious device or IP activity, unauthorised wallet changes, and unusual withdrawal behaviour.

10. Third-Party Providers

Where the Company uses third-party crypto payment processors, custodians, exchanges, or blockchain analytics providers, such providers will be subject to due diligence and periodic review.

The Company will assess, where relevant, the provider's licensing or registration status, AML/CFT and sanctions controls, information security standards, reputation, jurisdictional exposure, contractual protections, reporting capabilities, and business continuity arrangements.

The Company remains responsible for meeting its regulatory obligations and will maintain appropriate oversight over third-party providers.

11. Record Keeping and Reporting

The Company will maintain records of cryptocurrency-related activity, including customer verification records, wallet addresses, transaction hashes, screening results, source of funds evidence, internal reviews, escalations, customer communications, and management decisions.

Records will be retained in accordance with applicable legal and regulatory requirements and made available to the CGA, FIU Curaçao, or other competent authorities upon lawful request.

Any unusual or suspicious activity will be reviewed by the MLRO / Compliance Officer and, where required, reported to the relevant authority in accordance with applicable law and internal reporting procedures.

12. Review

This Policy will be reviewed at least annually and whenever there is a material change to the Company's business model, supported crypto-assets, payment providers, applicable laws, regulatory expectations, risk profile, or identified control weaknesses.

Any material changes to this Policy must be approved by senior management.

Approved by:

Jevgenijs Curikovs

Director, Jevgenijs Curikovs
For and on behalf of Universe B Games B.V.



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

29.06.2026