

Crypto Usage Risk Policy for iGaming B2C Operator

I. Purpose and Scope

This policy defines the principles, controls, and procedures governing the acceptance, use, and management of cryptocurrency transactions within the company's iGaming platform. It applies to all business units, employees, customers, and third-party partners involved in crypto-related operations.

II. Objectives

- Prevent and mitigate money laundering (ML), terrorist financing (TF), and fraud risks.
- Ensure compliance with applicable regulations, including AML/CFT obligations.
- Maintain the integrity of gaming operations and protect the company's reputation.
- Ensure that crypto acceptance aligns with responsible gaming principles and customer protection standards.

III. Definitions

- Virtual Asset (VA): A digital representation of value that can be transferred or exchanged digitally (e.g., Bitcoin, Ethereum).
- VASP (Virtual Asset Service Provider): A regulated entity facilitating the exchange, transfer, or custody of virtual assets.
- Fiat Conversion Partner: A third-party provider used to convert crypto to fiat or vice versa.
- Wallet Address: The unique identifier associated with a crypto wallet.

IV. Risk Assessment and Categorization

The operator will conduct a Crypto Risk Assessment (CRA) covering jurisdictional risks, VASP risks, wallet type, transaction patterns, and source of funds. A Crypto Risk Register will document risk levels and controls.

V. Permitted Cryptocurrencies

Only approved cryptocurrencies (e.g., BTC, ETH, USDT, USDC) will be accepted based on market capitalization, liquidity, and blockchain traceability. Privacy coins are prohibited.

VI. Onboarding and KYC Requirements

All crypto users must undergo full KYC. Enhanced Due Diligence (EDD) is required for high-risk customers, PEPs, and high-risk jurisdictions.

VII. Transaction Monitoring

Blockchain analytics tools must screen wallet addresses and transactions for illicit activity. Real-time alerts, transaction limits, and velocity thresholds apply.

VIII. Conversion and Custody

Crypto deposits are converted to fiat via regulated VASPs. The company will not hold crypto unless board-approved. Custodial wallets must be managed by licensed providers.

IX. Withdrawals

Withdrawals only allowed to verified wallets. Tracing required for destination wallets. EDD and manual review for large or unusual withdrawals.

X. Record Keeping

Maintain records of wallets, transaction IDs, KYC/EDD, and screening results for at least 5 years or per AML regulations.

XI. Reporting Obligations

File Suspicious Activity Reports (SARs/STRs) for suspicious crypto activity and notify regulators where required.

XII. Third-Party Partners

Partner only with regulated VASPs with strong AML frameworks. Conduct periodic due diligence and risk scoring of partners.

XIII. Staff Training and Awareness

Mandatory annual training for compliance, payments, and support staff on crypto AML risks, red flags, and procedures.

XIV. Governance and Oversight

Compliance Officer oversees crypto operations. A Crypto Risk Committee reviews incidents quarterly. Annual independent audit required.

XV. Incident Response and Policy Breach

Breaches must be reported to Compliance. Incident reviews determine remedial action and possible regulatory disclosure.

XVI. Continuous Improvement

Monitor regulatory and technological changes. Update policy annually or as needed.