

Pelican Entertainment B.V.

Registration Number: 134359

Registered Address: Dr. H. Fergusonweg 1, Curaçao

Comprehensive Risk Policy for Cryptocurrency Usage

Approved By:

Pelican Entertainment B.V. Board of Directors

Effective Date: 09/12/2024



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

1. Purpose and Scope

This policy establishes a structured approach for managing risks associated with cryptocurrency use within Pelican Entertainment B.V. ("the Company"). By providing clear guidelines for secure operations, it ensures that cryptocurrency transactions are carried out transparently, securely, and in compliance with legal and regulatory requirements.

The policy applies to all levels of the organization, including employees, contractors, subsidiaries, and third-party partners. It encompasses activities such as cryptocurrency deposits, withdrawals, storage, and payouts, with a focus on mitigating risks and ensuring compliance with applicable regulations.

Key Objectives:

- Protect the financial and operational integrity of cryptocurrency-related processes.
 - Ensure full compliance with Curaçao regulations and international standards.
 - Minimize exposure to market volatility, financial crime, and cybersecurity threats.
 - Establish a culture of accountability and continuous improvement.
-

2. Legal and Regulatory Compliance

Pelican Entertainment B.V. adheres to a robust framework of legal and regulatory standards. Compliance is integral to the Company's cryptocurrency operations, ensuring that all activities align with Curaçao's laws and global best practices.

- **Local Regulations:**
 - **Gaming Board Curaçao Requirements:** Cryptocurrency use in gaming operations complies with licensing standards.
 - **National Ordinances (NORUT and NOIS):** Mandates reporting unusual transactions and verifying client identities.
- **International Standards:**
 - **FATF Recommendations:** Implements risk-based measures for managing Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs).
 - **EU Directives (AMLD5 and AMLD6):** Guides identity verification, recordkeeping, and suspicious activity reporting.
 - **Basel Committee Guidelines:** Establishes global benchmarks for mitigating risks associated with digital assets.

Compliance Process:

1. **Continuous Monitoring:** The Compliance Officer reviews updates in legal frameworks.
2. **Documentation:** Comprehensive records of all cryptocurrency transactions are maintained for five years.
3. **Auditing:** Internal and external audits verify compliance with regulations and policies.

Key Elements in Compliance Scheme:

- **KYC Requirements:**
 - Mandatory identity verification for all customers.
 - Use of government-issued identification and proof of address.
- **AML Controls:**
 - Enhanced Due Diligence (EDD) for high-risk transactions.
 - Automated systems to flag unusual activities.

Visual Scheme: Compliance Workflow

1. **Transaction Initiation** →
2. **KYC Verification** →
3. **Transaction Screening for Risks** →
4. **Flagging Suspicious Activities** →
5. **Regulatory Reporting (FIU Curaçao)**

3. Governance and Oversight

Effective governance is essential to the successful implementation of this policy. The Company has clearly defined roles and responsibilities to ensure accountability and operational excellence in cryptocurrency management.

Key Governance Roles:

- **Board of Directors:**
 - Provides strategic oversight and approves cryptocurrency policies.
 - Reviews quarterly reports on compliance and risk management.
- **Compliance Officer:**
 - Acts as the primary liaison with regulatory bodies.
 - Oversees AML/CFT measures and ensures regulatory adherence.
- **Risk Management Committee:**
 - Evaluates cryptocurrency-specific risks and develops mitigation strategies.
 - Conducts quarterly reviews of transaction records and operational risks.
- **Internal Audit Team:**
 - Performs quarterly assessments of cryptocurrency processes.
 - Identifies vulnerabilities and recommends corrective actions.

Governance Flow Diagram:

1. **Policy Design by Risk Management Committee** →
2. **Policy Approval by Board of Directors** →
3. **Implementation by Compliance and Operational Teams** →
4. **Quarterly Audits by Internal Audit Team** →
5. **Findings Reported to Board**

4. Risk Assessment and Mitigation

4.1 Market Volatility Risks

The high volatility of cryptocurrency prices poses a significant challenge. To address this, the Company utilizes stablecoins such as USDC or USDT for high-value transactions, reducing exposure to price fluctuations. Additionally, a dynamic pricing system ensures that transactions are adjusted in real time to reflect market trends.

Mitigation Measures:

- Daily market analysis by financial experts.
 - Real-time pricing adjustments for transactions.
 - Review and approval of high-value transactions by the Risk Management Committee.
-

4.2 Regulatory Risks

Regulatory changes in cryptocurrency legislation require constant vigilance. The Compliance Officer tracks global regulatory developments, ensuring the Company remains compliant with evolving requirements. Detailed transaction records and KYC data are securely archived for at least five years to meet audit and regulatory standards.

Steps to Mitigate Regulatory Risks:

1. Monthly compliance reviews.
 2. Immediate updates to policies based on regulatory changes.
 3. Communication of updates to all relevant employees.
-

4.3 AML/CFT and Fraud Risks

The pseudo-anonymous nature of cryptocurrencies increases the risk of financial crimes such as money laundering and fraud. The Company employs advanced transaction monitoring systems to detect suspicious patterns and ensure compliance with AML regulations.

Measures to Prevent Financial Crimes:

- Mandatory KYC checks before processing transactions.
 - Blockchain tracing for high-risk transactions.
 - Automated flags for transactions exceeding predefined thresholds.
-

4.4 Cybersecurity Risks

Cryptocurrencies are vulnerable to hacking, phishing, and unauthorized access. To mitigate these risks, Pelican Entertainment B.V. employs a dual-wallet system, with hot wallets used for daily operations and cold wallets for long-term storage. Multi-signature access controls and two-factor authentication add additional layers of security.

Cybersecurity Framework:

- **Cold Wallets:** Offline storage with multi-signature access.
 - **Hot Wallets:** Secured by two-factor authentication and real-time monitoring.
 - **Incident Response:** Structured protocols for identifying and mitigating breaches.
-

5. Training and Awareness

Training is a vital component of the Company's cryptocurrency risk management strategy. All employees handling cryptocurrency transactions undergo mandatory training programs that cover AML/CFT compliance, secure wallet management, and fraud detection. Specialized training is provided for compliance personnel, focusing on blockchain analytics and risk assessment techniques.

Training Structure:

1. **Initial Training:** Comprehensive onboarding for new employees.
 2. **Specialized Modules:** Tailored for compliance and operational teams.
 3. **Refresher Courses:** Conducted bi-annually to address new threats.
 4. **Assessments:** Regular evaluations to ensure knowledge retention.
-

6. Monitoring, Reporting, and Continuous Improvement

Monitoring systems analyze cryptocurrency transactions in real time, identifying unusual patterns or behaviors. The Compliance Team reviews flagged transactions, escalating suspicious cases to the appropriate regulatory authorities. Monthly compliance reports summarize flagged activities and resolutions, forming the basis for quarterly audits and annual reviews.

Improvement Process:

- Findings from audits are incorporated into policy updates.
 - Emerging risks are addressed through new controls and strategies.
 - Employee feedback is integrated into training programs for better engagement.
-