

1. Introduction

This document outlines the integrated risk management and anti-money laundering policies of WoT NV as they pertain to the handling of cryptocurrencies. Our commitment is to uphold the highest standards of compliance as required by the Gaming Control Board, ensuring that our operations not only meet but exceed the regulatory expectations for financial security and integrity in cryptocurrency transactions.

2. Scope and Applicability

This policy governs all cryptocurrency-related activities within WoT NV, including trading, exchanges, storage, and usage. It applies to all our employees, contractors, and subsidiaries engaged in operations that involve digital currencies.

3. Definitions

- **Cryptocurrency:** A digital currency that uses cryptographic technology for secure financial transactions.
- **Blockchain:** A decentralized digital ledger that records all cryptocurrency transactions across a network of computers.
- **AML (Anti-Money Laundering):** Legal controls that require financial institutions to prevent, detect, and report money laundering activities.
- **Risk:** The exposure to adverse consequences in our financial position or reputation.

4. Risk Identification

Key risks associated with the use of cryptocurrencies include:

- **Market Risk:** Extreme volatility in cryptocurrency valuations.
- **Regulatory Risk:** The evolving legal landscape and its impacts on cryptocurrency practices.
- **Security Risk:** Potential breaches in our digital infrastructure leading to theft or loss of assets.
- **Operational Risk:** Inadequacies in internal processes or controls that could lead to financial losses.

5. Risk Assessment

Risks are evaluated for their likelihood and impact, utilizing both qualitative assessments and quantitative metrics. This assessment informs the development of our mitigation strategies and shapes our continuous monitoring efforts.

6. Risk Mitigation Strategies

To address the identified risks, we implement:

- **Robust Security Measures:** Including advanced cryptographic techniques, segregated wallets, and regular security audits.
- **Stringent Compliance Measures:** Ensuring adherence to AML, KYC (Know Your Customer), and other regulatory requirements.
- **Employee Training and Awareness:** Continuous education on best practices and emerging risks in cryptocurrency operations.
- **Financial Exposure Limits:** Set thresholds for cryptocurrency holdings to manage volatility risks.

7. Anti-Money Laundering Policies

We adopt rigorous AML protocols to prevent illicit activities:

- **Transaction Monitoring:** Real-time analysis to detect suspicious patterns indicative of money laundering.
- **Customer Due Diligence:** Thorough verification processes to understand the nature of our customers' activities and the risks they pose.
- **Reporting Obligations:** Immediate reporting of suspicious activities to appropriate authorities in accordance with legal and regulatory guidelines.

8. Monitoring and Reporting

Our dedicated compliance team continuously monitors adherence to these policies, ensuring effective implementation and immediate response to policy breaches. Compliance findings are reported to the Board of Directors quarterly.

9. Review and Update of Policy

This policy is reviewed annually or following significant regulatory changes or major incidents. This ensures our practices remain at the forefront of industry standards and regulatory requirements.

10. Compliance and Enforcement

Violations of this policy are met with strict penalties, up to and including termination of employment, legal action, and regulatory notification. We maintain a zero-tolerance approach to non-compliance, underscoring our commitment to integrity and ethical conduct.