CRYPTO RISK MANAGEMENT POLICIES
FOR NON-STABLE CRYPTOCURRENCIES

Date: 20.10.2024

1. INTRODUCTION

This policy outlines the measures to identify, manage, and mitigate risks associated with the acceptance of non-stable cryptocurrencies on the company's platform. These policies align with regulatory standards and best practices to ensure the safety, security, and integrity of financial transactions. The document aims to provide a robust framework for addressing the challenges posed by the unique characteristics of non-stable cryptocurrencies.

The acceptance of non-stable cryptocurrencies introduces both opportunities and challenges. This policy emphasizes a structured approach to mitigate risks and maximize the potential benefits of cryptocurrency integration while adhering to legal and ethical standards. By understanding and addressing these risks, the company aims to provide a seamless, secure, and transparent user experience while meeting its legal obligations.

2. SCOPE

This policy applies to all operations involving non-stable cryptocurrencies on the platform, including deposits, withdrawals, internal transfers, and any transactions conducted with external entities. It covers the roles and responsibilities of all employees, partners, and service providers involved in cryptocurrency management. The policy also applies to the technological infrastructure supporting crypto operations and the implementation of security measures to protect digital assets.

This scope ensures that all stakeholders understand their roles in mitigating risks and complying with legal obligations. The policy also extends to ongoing relationships with vendors, ensuring third-party compliance with risk management protocols.

3. RISK IDENTIFICATION

The primary risks associated with non-stable cryptocurrencies include:

- **Price Volatility:**
  - Rapid fluctuations in value could significantly impact business revenue, user experience, and operational budgeting.
  - Potential for losses if cryptocurrencies are not converted to stable assets promptly.
  - Volatility may affect user trust and willingness to engage with the platform.
- **Fraud and Financial Crime:**
  - Non-stable cryptocurrencies offer anonymity, increasing the risk of illicit activities like money laundering (ML), terrorist financing (TF), and fraud.
  - High transaction speeds may make it challenging to intervene in real-time during suspicious activity.

    - Emerging criminal techniques targeting blockchain technologies require ongoing vigilance.
- **Regulatory Compliance:**
    - Compliance challenges arise from differing regulatory requirements in various jurisdictions.
    - Failing to comply with AML and CTF obligations can lead to legal penalties and reputational damage.
    - The evolving nature of cryptocurrency regulations necessitates constant monitoring and adaptability.
- **Security Risks:**
    - Increased susceptibility to cyber threats such as hacking, phishing, ransomware attacks, and insider threats.
    - Vulnerability of hot wallets to unauthorized access.
    - Potential exploitation of system vulnerabilities by attackers.
- **Liquidity Risks:**
    - Difficulty in ensuring sufficient liquidity for large withdrawal requests during periods of high market volatility.
    - Potential delays in converting cryptocurrencies to fiat or stablecoins.
    - Dependency on external liquidity providers, which may pose additional risks.

4. RISK MANAGEMENT FRAMEWORK

The Company's platform adopts the following measures to manage and mitigate risks:

4.1 Price Volatility Management

- Implement real-time monitoring of cryptocurrency prices using advanced algorithms and analytics.
- Utilize automated conversion tools to convert non-stable crypto into fiat or stablecoins immediately upon deposit, minimizing exposure to volatility.
- Establish pre-defined thresholds for cryptocurrency holdings, triggering automated conversion or other actions when exceeded.
- Maintain a diversified portfolio of cryptocurrencies to spread risks.
- Incorporate hedging strategies to minimize losses during extreme market fluctuations.

4.2 Fraud and Financial Crime Prevention

- Adopt a comprehensive Know Your Customer (KYC) and Customer Due Diligence (CDD) process to ensure the users are verified with government-issued IDs and proof of address.
- Conduct enhanced due diligence (EDD) for high-risk users, including Politically Exposed Persons (PEPs).
- Utilize blockchain analytics tools to:

    - Track and analyze transaction histories.
    - Identify patterns and behaviors associated with fraudulent or illicit activities.
    - Monitor wallets linked to known criminal activities.
- Require users to link accounts with identifiable payment methods for withdrawal verification.
- Establish clear protocols for reporting suspicious transactions to Curacao's Financial Intelligence Unit (FIU).
- Ensure alignment with global data privacy standards during data collection and reporting processes.

4.3 Regulatory Compliance

- Align AML/CTF policies with Curacao regulations, FATF recommendations, and other applicable international standards.
- Develop internal compliance teams to monitor evolving regulations and ensure proactive adherence.
- Implement automated systems for generating reports required by regulatory bodies, including transaction logs and risk assessments.
- Engage regularly with legal advisors to remain informed about regulatory changes and potential implications.

4.4 Security Measures

- Utilize multi-signature authentication for accessing and transferring funds from hot and cold wallets.
- Store the majority of funds in offline cold wallets, segmented by operational need.
- Implement advanced cybersecurity measures, including:
    - Firewalls and intrusion detection systems.
    - Regular updates to software and systems to patch vulnerabilities.
    - Role-based access controls for sensitive operations.
- Conduct regular security audits, penetration tests, and system integrity checks.
- Establish redundancy in security measures, such as backup systems and alternative wallets.
- Educate employees on recognizing phishing attempts, social engineering, and other threats.

4.5 Liquidity Management

- Partner with reliable and reputable cryptocurrency exchanges to ensure access to liquidity.
- Maintain a reserve of fiat currencies and stablecoins to cover user withdrawals during market volatility.
- Develop contingency plans for liquidity crises, including emergency funding sources and temporary withdrawal caps.

- Use predictive analytics to anticipate periods of high liquidity demand.

5. INCIDENT RESPONSE PLAN

- Establish an incident response team with representatives from compliance, IT, legal, finance and operations departments.
- Develop a detailed protocol for managing incidents, including:
  - Identifying and isolating affected systems.
  - Communicating with stakeholders and users transparently.
  - Coordinating with law enforcement and regulators as necessary.
- Test the incident response plan regularly through simulations and drills.
- Include post-incident reviews to identify and implement improvements.

6. GOVERNANCE AND OVERSIGHT

- Assign a Crypto Risk Manager to oversee risk management policies, their implementation, and regular updates.
- Establish a Crypto Risk Committee to provide strategic oversight and review quarterly reports on risk management activities.
- Set up whistleblowing channels for employees to report potential security breaches or compliance issues confidentially.
- Regularly evaluate the effectiveness of governance structures and revise as needed.

7. TRAINING AND AWARENESS

- Provide mandatory training for all employees on:
  - Cryptocurrency-specific risks.
  - AML/CTF compliance.
  - Best practices for cybersecurity and fraud prevention.
- Conduct regular refresher courses to ensure employees are updated on the latest threats and regulatory changes.
- Offer user education programs to raise awareness about fraud, phishing, and other risks associated with non-stable cryptocurrencies.
- Host periodic webinars and workshops featuring experts in crypto risk management.

8. MONITORING AND REPORTING

- Implement continuous monitoring systems leveraging artificial intelligence to detect anomalies and flag high-risk transactions.
- Conduct regular audits of cryptocurrency transactions to ensure compliance and identify weaknesses.
- Generate detailed monthly reports on cryptocurrency usage, including:

  - Volume and value of transactions.
  - Number and nature of flagged transactions.
  - Metrics on compliance performance and security incidents.
- Share high-level summaries with stakeholders to maintain transparency and trust.

9. POLICY REVIEW

- Conduct annual reviews of this policy, or more frequently if significant operational, regulatory, or market changes occur.
- Involve external experts in policy reviews to ensure the framework remains robust and aligned with global best practices.
- Document changes to the policy and communicate updates to all stakeholders.
- Benchmark policies against industry leaders to identify areas for improvement.

10. CONCLUSION

By implementing these comprehensive risk management policies, the company seeks to create a secure and compliant environment for accepting non-stable cryptocurrencies. The approach prioritizes customer trust, regulatory adherence, and operational resilience while leveraging the benefits of cryptocurrency integration. This policy reflects the organization's commitment to proactive risk management and innovation in the rapidly evolving digital asset landscape.

In conclusion, the company remains committed to continuously improving its crypto risk management framework by embracing emerging technologies, enhancing internal controls, and fostering a culture of compliance and security. Through these efforts, the company aims to maintain a leadership position in the industry, ensuring long-term success and a robust operational environment that aligns with the evolving needs of users and stakeholders.