



TRUSTDICE CRYPTO RISK POLICY

1. Introduction

This Crypto Risk Policy outlines the key risks associated with cryptocurrency use in the context of TrustDice and establishes a framework for managing these risks. It applies to all employees, contractors, and other stakeholders involved in the company's operations.

2. Scope

This policy covers all aspects of cryptocurrency use within the company, including:

- **Investments:** Investing in and holding cryptocurrencies as part of the company's treasury management strategy.
- **Payments:** Accepting and processing payments in cryptocurrencies for goods and services.
- **Internal operations:** Using cryptocurrencies for internal transactions, such as payroll or vendor payments.
- **Third-party relationships:** Engaging with cryptocurrency exchanges, wallets, and other service providers.

3. Risk Identification

The following are the key risks associated with cryptocurrency use in the context of the company:

- **Price volatility:** Cryptocurrencies are subject to significant price fluctuations, which can impact the value of the company's investments and holdings.
- **Security breaches:** Cryptocurrency exchanges and wallets are vulnerable to hacking and theft.
- **Regulatory uncertainty:** The regulatory landscape for cryptocurrencies is constantly evolving, which could impact the legality of the company's operations.

- **Fraud and money laundering:** Cryptocurrencies can be used for illicit activities, such as fraud and money laundering.
- **Operational challenges:** Managing cryptocurrency transactions can be complex and resource-intensive.

4. Risk Management

To mitigate the risks identified above, the company will implement the following measures:

- **Price volatility:**
 - Diversify the company's cryptocurrency holdings across different assets.
 - Implement stop-loss orders to limit potential losses.
 - Regularly monitor market conditions and adjust strategies accordingly.
- **Security breaches:**
 - Use reputable and secure cryptocurrency exchanges and wallets.
 - Implement strong security protocols, including multi-factor authentication and encryption.
 - Conduct regular security audits.
- **Regulatory uncertainty:**
 - Stay informed about regulatory developments and adjust operations accordingly.
 - Engage with regulators and industry bodies to promote responsible cryptocurrency use.
- **Fraud and money laundering:**
 - Implement KYC/AML procedures to verify the identity of counterparties and monitor transactions for suspicious activity.
 - Report any suspected fraudulent or illegal activity to the relevant authorities.

- **Operational challenges:**

- Develop efficient processes for managing cryptocurrency transactions.
- Invest in technology and resources to support cryptocurrency operations.

5. Responsibilities

All employees, contractors, and other stakeholders are responsible for adhering to this Crypto Risk Policy. The company's management team is responsible for overseeing the implementation and effectiveness of this policy.

6. Review and Update

This Crypto Risk Policy will be reviewed and updated regularly to reflect changes in the cryptocurrency landscape and the company's operations.