

Introduction

This document outlines the Crypto Risk Policy for Games & More BV, hereinafter referred to as the "Operator". As cryptocurrencies become more prevalent in the online gaming industry, it is imperative to establish protocols and guidelines to manage associated risks effectively.

Purpose

The purpose of this policy is to identify, assess, and mitigate risks related to the use of cryptocurrencies within the operations. It aims to ensure the security, integrity, and reliability of all cryptocurrency transactions while providing a seamless and safe experience for our customers.

Scope

This policy applies to all employees, contractors, and stakeholders involved in the cryptocurrency operations. It encompasses the use of cryptocurrencies for deposits, withdrawals, and any other related activities.

Risk Identification and Assessment

- a. **Volatility Risk:** Cryptocurrency markets are highly volatile and subject to rapid price fluctuations. The Operator acknowledges this risk and advises customers accordingly.
- b. **Security Risk:** Cryptocurrencies are susceptible to hacking, fraud, and theft. The Operator employs robust security measures to safeguard customers' funds and personal information.
- c. **Regulatory Risk:** Regulatory frameworks surrounding cryptocurrencies vary by jurisdiction and may change over time. The Operator monitors regulatory developments and adjusts its policies and procedures accordingly.
- d. **Operational Risk:** Operational errors or technical glitches may occur during cryptocurrency transactions, leading to potential financial losses or customer dissatisfaction. The Operator implements stringent controls and conducts regular audits to mitigate such risks.

Risk Mitigation Strategies

- a. **Volatility Management:** The Operator offers real-time pricing information and encourages customers to exercise caution when trading cryptocurrencies. It may also impose limits or restrictions on cryptocurrency transactions during periods of extreme volatility.
- b. **Security Measures:** The Operator employs industry-leading security protocols, including encryption, multi-factor authentication, cold storage solutions, and regular security audits. It educates customers on best practices for securing their cryptocurrency holdings.
- c. **Regulatory Compliance:** The Operator adheres to all applicable laws and regulations governing cryptocurrency transactions, including anti-money laundering (AML) and know-

your-customer (KYC) requirements. It maintains open communication with regulatory authorities and seeks legal counsel as needed.

d. Operational Controls: The Operator implements robust internal controls and procedures to minimize the risk of operational errors or fraud. It conducts regular training sessions for staff members involved in cryptocurrency transactions and maintains contingency plans for handling unforeseen events.

Customer Communication and Education

The Operator provides clear and concise information to customers regarding the risks associated with cryptocurrency transactions. It offers educational resources, tutorials, and support channels to help customers make informed decisions and navigate the cryptocurrency landscape safely.

Monitoring and Review

The Operator continuously monitors its cryptocurrency operations and evaluates the effectiveness of risk mitigation strategies. It conducts regular reviews and updates to this policy in response to emerging threats, regulatory changes, or lessons learned from past incidents.

Conclusion

By adhering to this Crypto Risk Policy, the Operator demonstrates its commitment to maintaining the highest standards of security, compliance, and customer satisfaction in all cryptocurrency-related activities. All employees and stakeholders are expected to familiarize themselves with this policy and adhere to its provisions at all times.