

CRYPTO CURRENCY RISK
MANAGEMENT POLICY

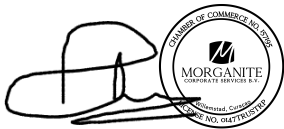
Agenics N.V.

Registration number 149347

VERSION HISTORY

Version	Version Date	Author	Summary of Changes
1.0	September 2025	Compliance Department	

APPROVALS



Name	Title	Date of Approval	Version
Morganite Corporate Services B.V.	Managing Director	09.05.2025	1.0

Contents

1.	Introduction	3
2.	Regulatory Compliance	3
3.	Scope of Use	3
4.	Definitions.....	3
5.	Accepted Cryptocurrencies.....	4
6.	Unaccepted Cryptocurrencies	4
7.	Payment Processing.....	5
8.	Customer Identification and Wallet Verification	5
9.	Wallet Security.....	5
10.	Risk Categories	5
11.	Policy Updates	6

1. Introduction

This Cryptocurrency Policy sets forth the terms under which Agenics N.V. (the Company) accepts cryptocurrency as a form of payment for goods and services available on its gaming platform. As part of the Company's commitment to innovation and user convenience, this policy supports the integration of decentralized financial technologies into its operations. The objective is to provide users with secure and efficient alternative payment methods, while ensuring the Company maintains full compliance with all applicable legal and regulatory frameworks. Additionally, this policy is intended to safeguard the Company's assets and uphold transparency and accountability in its financial operations, thereby fostering confidence among users, partners, and regulatory bodies.

2. Regulatory Compliance

The Company acknowledges the evolving legal landscape surrounding cryptocurrency and is fully committed to complying with all applicable local and international laws and regulations. This includes, but is not limited to, financial services registration, reporting obligations, anti-money laundering (AML) measures, and counter-terrorism financing (CTF) protocols. The compliance department in conjunction with the finance department shall be responsible for continuously monitoring legal developments and adapting internal policies and procedures accordingly. The Company retains full discretion to refuse or halt any transaction suspected of involving illicit activity or failing to meet compliance standards. This proactive approach ensures that the Company operates in a lawful and ethical manner while mitigating regulatory and reputational risk.

3. Scope of Use

Cryptocurrency payments on the Company's platform are permitted for specific use cases, including:

- Placing wagers or stakes on games of chance;
- Purchasing in-game promotional material that enhance user experience;
- Acquiring other digital services or assets explicitly offered on the platform.

4. Definitions

Cryptocurrency: A digital asset designed to work as a medium of exchange using cryptography to secure transactions on a decentralized ledger.

Wallet Screening: The process of analyzing blockchain addresses using forensic tools to identify links to illicit activities, including scams and dark web connections (as promoted by Reclaim My Losses tools that "screen more than 100 crypto assets, identify wallet owners, and track the source and destination of payments").

High-Risk Customer: Any individual or entity from a sanctioned jurisdiction, exhibiting suspicious behavior, or using privacy-enhancing technologies.

VASP: Virtual Asset Service Providers, entities facilitating the exchange or storage of crypto assets.

KYC : Know Your Customer

AML/CFT: Anti Money Laundering/ Counter-terrorism financing

BTC: Bitcoin

ETH: Etheurum

LTC: Litecoin

XRP: Ripple

5. Accepted Cryptocurrencies

The Company maintains a clear and conservative policy on acceptance of cryptocurrencies. To mitigate risks related to anonymity, fraud, and regulatory uncertainty only specific cryptocurrencies are permitted on the platform.

The Company evaluates supported cryptocurrencies based on factors such as market adoption, regulatory clarity, technical reliability, and liquidity. This list may be amended at any time in response to operational needs, market conditions, or legal obligations.

Approved Cryptocurrencies are: Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH), Ripple (XRP) and USDC. These offer high market liquidity, are supported by most regulated exchanges and can be subjected to forensic blockchain analysis.

Token Risk Evaluation: All new tokens and coins must undergo an internal vetting process including a technical audit, liquidity analysis, exchange availability and sanction screening using tools such as Chainalysis or Elliptic.

Additional cryptocurrencies may be accepted in future, subject to operational considerations and market demand. The Company reserves the right to add or remove supported cryptocurrencies at any time without prior notice.

6. Unaccepted Cryptocurrencies

To maintain regulatory compliance and mitigate risk, the Company prohibits use of certain cryptocurrencies that; deems unsuitable for its platform, are privacy-focused coins which obscure transaction history, tokens with limited liquidity or high volatility that pose settlement risks and cryptocurrencies with unclear legal status or association with illicit activities.

Prohibited currencies are but are not limited to:

Monero (XMR), Zcash (ZEC), and Dash (DASH). These coins are designed to obscure transactional data and are widely used in darknet markets. This prohibition aligns with the FATF and EU recommendations regarding untraceable virtual assets.

NFTs and DeFi tokens are not permitted due to high volatility and frequent involvement in scam schemes.

The list of prohibited digital assets is dynamic and may be updated periodically. These exclusions are informed by internal risk assessments, industry trends, and evolving guidance from financial

regulators. By implementing these limitations, the Company ensures it can meet AML and Know Your Customer (KYC) obligations effectively.

7. Payment Processing

All cryptocurrency transactions are processed through a reputable third-party payment gateway, which facilitates secure and compliant handling of digital funds. These gateways convert incoming cryptocurrency payments into fiat currencies such as USD or Euro in real-time, based on the prevailing exchange rate at the time of transaction confirmation. This process ensures price consistency and operational efficiency for the Company. Any applicable transaction fees, including network fees or gateway processing charges, will be clearly communicated to the user during the checkout process and must be paid by the user. The Company does not assume responsibility for fees imposed by external wallets or exchanges.

8. Customer Identification and Wallet Verification

To meet AML/CTF obligations and ensure the security of crypto transactions, the Company enforces a rigorous customer and wallet verification process:

- **KYC (Know Your Customer):** All users who wish to transact in crypto must complete identity verification. This includes government-issued photo ID, proof of address, and liveness or biometric verification.
- **Wallet Ownership Verification:** Customers must submit the public address of the wallet they intend to use.

The wallet must:

- Be non-custodial (i.e., not controlled by exchanges or third parties).
- Match the customer's identity as verified through blockchain ownership proofs (e.g., micro-deposit with verification signature).

9. Wallet Security

The Company employs stringent security measures to protect its cryptocurrency holdings. Operational funds needed for day-to-day transactions are stored in hot wallets protected by multi-signature protocols and other access controls. Most of the Company's funds are maintained in cold wallets - offline storage solutions with access restricted to a limited number of senior authorized personnel. These practices align with industry best standards for safeguarding digital assets and minimize the risk of hacking, theft, or unauthorized access. Regular audits and security reviews are conducted to ensure the continued integrity of wallet infrastructure.

10. Risk Categories

AML/CFT Risk

Cryptocurrency's pseudonymous nature allows transactions to be made without immediate identification. FATF highlights this as a risk for money laundering and terrorist financing. Therefore, the Company mandates full KYC for all users transacting in cryptocurrencies.

Fraud Risk

Fraudulent schemes like giveaway scams, phishing, and social engineering are extensively described in scam literature. As noted, "Fraudsters impersonate celebrities or well-known investors" to gain trust. Our systems actively flag behavioral anomalies and detect account takeover patterns through multi-layered monitoring.

Volatility Risk

As altcoins can behave like "illiquid penny stocks" subject to "pump and dump" manipulation, the Company accepts most likely stablecoins (e.g., USDT). This stabilizes the treasury and minimizes customer disputes due to exchange fluctuations.

Regulatory Risk

Different jurisdictions interpret crypto legality variably. Agenics N.V. monitors developments across the FATF, EU, and Caribbean Financial Action Task Force.

11. Policy Updates

This policy shall be reviewed:

- Annually
- Upon major regulatory change
- In response to internal incidents or audit findings

Policy amendments are prepared by the Compliance Officer and are binding on all personnel.