

CRYPTOCURRENCY RISK MANAGEMENT POLICY

of Goodwin N.V.

This document outlines the risk mitigation measures, compliance requirements, and security protocols adopted by Goodwin N.V. in connection with the use of cryptocurrencies within its regulated online gaming operations.

Version 1.0 | Effective: April 15, 2025

Signed by:


Vladyslav Nebrat

Approved on 07.31.2025
Morganite Corporate Services B.V.
Managing Director



1. Introduction

Cryptocurrency has revolutionized digital transactions, offering anonymity, speed, and decentralization. However, these advantages also present unique risks, particularly in high-risk industries such as online gaming. Goodwin N.V., licensed and regulated in Curaçao (hereinafter - the “Company”), has adopted this Cryptocurrency risk management policy to ensure responsible and compliant use of cryptocurrency within its operations (hereinafter - the “Policy”).

This Policy aims to align with international standards, including FATF Recommendations, EU AML Directives, and cybersecurity guidelines, while also addressing fraud prevention measures. As outlined in that document, crypto transactions are susceptible to "phishing, social engineering, and account takeover attempts" and require strict monitoring to mitigate associated risks.

2. Scope

This policy applies to all departments and personnel of Goodwin N.V. involved in crypto-related operations. It includes:

- The onboarding of customers who deposit or withdraw funds in cryptocurrency.
- Internal teams conducting due diligence and transaction monitoring.
- Third-party providers offering wallet services or blockchain analytics.
- Compliance with security controls outlined in cybersecurity protocols, such as vulnerability assessments, patch management, and encryption.

3. 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.

4. Risk Categories

4.1 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, Goodwin N.V. mandates full KYC for all users transacting in crypto.

4.2 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.

4.3 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.

4.4 Regulatory Risk

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

5. Permissible Cryptocurrencies

Company Goodwin N.V. maintains a clear and conservative policy on accepted cryptocurrencies. To mitigate risks related to anonymity, fraud, and regulatory uncertainty, only specific cryptocurrencies are permitted on the platform:

- **Approved Assets:** Bitcoin (BTC), Ethereum (ETH), and Tether (USDT) on ERC-20 and TRC-20 networks. These assets offer high market liquidity, are supported by most regulated exchanges, and can be subjected to forensic blockchain analysis.
- **Prohibited Assets:** Goodwin N.V. strictly prohibits the use of privacy coins such as 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.
- **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.
- **NFTs and DeFi tokens** are not permitted due to high volatility and frequent involvement in scam schemes.

6. Customer Identification and Wallet Verification

To meet AML/CTF obligations and ensure the security of crypto transactions, Goodwin N.V. 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).
- **Wallet Screening:** All wallet addresses are screened against:
 - International sanctions lists (e.g., OFAC, UN, EU).
 - Dark web associations.
 - Risk ratings and fraud scores via blockchain analytics software.
- **High-Risk Flags:** If a wallet has any connection to ransomware, scams, or mixers, it is immediately flagged. The Compliance Department must perform Enhanced Due Diligence (EDD) before approval or rejection.

7. Transaction Monitoring

Goodwin N.V. employs a real-time blockchain monitoring and compliance engine to track all cryptocurrency activity:

- **Behavioral Pattern Analysis:** Transactions are monitored for structuring, layering, and high-frequency or unusual behavior.
- **Anomaly Detection:** Alerts are generated when transactions:
 - Originate from sanctioned jurisdictions.
 - Involve excessive use of DeFi, mixers, or privacy layers.
 - Involve large volumes inconsistent with customer profile.
- **Escalation Workflow:** Risk alerts are triaged based on severity. Medium and high-risk alerts are escalated to the AML Compliance Officer. Manual review includes verifying source of funds, transactional intent, and matching against customer profile.
- **Red Flags Referenced:** The Company's practice identifies frequent fraud tactics such as fake giveaways, wallet redirects, and impersonation — these are encoded as detection rules.
- **Reporting Obligations:** Where appropriate, suspicious transactions are reported in accordance with the Company's AML Policy.

8. Limits and Restrictions

To safeguard the platform and customers from financial crime, Goodwin N.V. imposes the following operational limits:

- **Deposit Limits:** Daily, weekly, and monthly deposit caps are configured based on a risk-based tiering system. Unverified users are not allowed to deposit in cryptocurrency.
- **иногда запрашивает пруфы (скриншот с кошелька) что кошель его**

- **Large Transaction Review:** Any transaction exceeding EUR 10,000 equivalent in crypto triggers enhanced scrutiny, including reconfirmation of source of funds and updated wallet screening.

9. Incident Management and Scam Prevention

In the event of a fraud alert, suspected scam, or cybersecurity breach involving cryptocurrency:

- **Immediate Freezing of Funds:** Affected wallet or account is frozen, and no further transactions are permitted until resolution.
- **Incident Review:** Compliance and IT teams perform joint analysis. Logs are reviewed, wallet activity traced, and external blockchain analytics engaged.
- **Victim Support:** Customers affected by scams receive assistance per internal policies, including documentation for law enforcement.
- **Government Reporting:** Incidents are reported to FIU and/or law enforcement within the timeline, established by law.
- **Post-Incident Action:** System logs are audited, and new detection rules are created to prevent recurrence.

10. Recordkeeping and Reporting

To maintain regulatory compliance and audit readiness:

- **Data Retention:** All crypto-related data — including KYC files, transaction records, wallet ownership proofs, screening logs, and compliance reviews — are retained securely for at least five (5) years.
- **Audit Trails:** All system actions are logged and protected against alteration. Logs are reviewed periodically to detect unauthorized access.
- **SAR Filings:** Suspicious Activity Reports are drafted and filed electronically with the regulator. Reports include full transaction hash data, IP addresses, wallet forensics, and supporting customer records.
- **Cybersecurity Integration:** Log retention follows guidance: "All logs of events and incidents to identify unusual patterns and behaviours should be audited".

11. Third-Party Crypto Processors

Goodwin N.V. may partner with external crypto service providers under strict contractual and technical safeguards:

- **VASP Due Diligence:** Only VASPs licensed in jurisdictions recognized by FATF and CFATF are eligible. Due diligence includes:
 - Company registration
 - Regulatory status
 - AML and security practices
- **Data Security Reviews:** Third-party partners must implement the same level of data protection, vulnerability testing, and system logging as internal systems. Independent audit reports may be requested.

- **Concentration Risk Management:** No single provider may process more than 50% of crypto volume.
- **Contingency Planning:** SLAs and fallback procedures are defined in the event of processor downtime, breach, or non-compliance.
- **Ongoing Monitoring:** Performance reviews and compliance audits are conducted bi-annually or upon incident.

13. Employee Training

The Company should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy extended to outsourced staff, vendors etc.

Training covers:

- Identification of scam red flags
- Blockchain transaction interpretation
- Escalation and reporting protocols

14. Policy Review and Updates

This policy shall be reviewed:

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

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

15. References

- FATF Guidance for Virtual Assets and VASPs
- EU AML Directives
- Curaçao Gaming License Framework
- Goodwin N.V. AML Policy