

Risk policy for cryptocurrency usage

Last updated 12.06.2025

Introduction

This policy is developed by Goodfly N.V., the company established under the laws of Curaçao, having its company registration number: 163359, and registered address at Abraham De Veerstraat 1.

Cryptocurrencies provide convenience and accessibility for our global customer base but also introduce unique risks, including those related to money laundering, terrorism financing, and sanction evasion.

As a responsible operator, Goodfly N.V. is committed to adhering to international standards for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT), as well as maintaining compliance with all relevant regulatory frameworks.

This document outlines the principles, procedures, and controls established to mitigate risks associated with cryptocurrency transactions while ensuring the integrity of our platform and protecting our stakeholders.

1. Purpose and Scope

1.1 Purpose

This policy aims to:

- Ensure the secure use of cryptocurrencies in online gambling transactions.
- Mitigate risks related to illegal activities, including money laundering, fraud, and terrorism financing.
- Maintain compliance with relevant legal and regulatory requirements across all jurisdictions where the company operates.
- Protect the reputation and financial stability of Goodfly N.V..

1.2 The scope of this policy extends to all employees, contractors, and third-party partners involved in cryptocurrency-related activities. It also encompasses all customers who use cryptocurrencies for deposits, withdrawals, or other transactions on the platform. Furthermore, this policy applies to all jurisdictions where Goodfly N.V. operates, ensuring adherence to both local and international legal frameworks.

1.3 To achieve its objectives, this policy aligns with key regulatory standards, including the Financial Action Task Force (FATF) recommendations, European Union

Anti-Money Laundering Directives (AMLDs) and specific gambling and cryptocurrency legislation in the countries where our business is active.

2. Risk Identification

Cryptocurrencies used in online gambling can be associated with many risks that Goodfly N.V. should consider. Below is a list of key risks:

2.1 Child exploitation

The risk of using cryptocurrencies to finance activities related to the sexual exploitation of children. Online gambling platforms can be used to transfer funds between participants in such crimes, using cryptocurrency to maintain anonymity. Addresses that have been flagged as being associated with child exploitation should be blocked immediately.

2.2 Dark market

Gambling platforms can accept funds earned through illegal black market transactions (sale of drugs, weapons, stolen data). This creates a significant reputational risk and possible fines for the company. Cryptocurrency addresses associated with black markets are easily identified through AML services and should be blocked immediately.

2.3 Dark service

Coins derived from serious crimes such as terrorist financing, human trafficking, or drug trafficking. Such services often use mixers to obfuscate transactions. Without proper monitoring, such transactions can end up with players or via P2P platforms.

2.4 Fraudulent exchange

Certain cryptocurrency exchanges operate without proper licensing or have been involved in illegal activities such as exit scams, money laundering, or fraud. Funds originating from such exchanges pose a significant risk, as they may be tied to illicit activities or subject to confiscation by authorities. If players use cryptocurrencies obtained from fraudulent exchanges, the company risks unknowingly facilitating illegal activities or facing financial losses due to asset freezes.

2.5 Mixer usage

Mixers, also known as tumblers, are services used to obscure the origin of cryptocurrency transactions by blending multiple inputs from different users. While mixers may have legitimate use cases, they are predominantly associated with illegal

activities, such as money laundering or fraud. Players using mixers to fund gambling accounts may be attempting to launder funds, exposing the platform to legal and reputational risks.

2.6 Ransom

Ransomware attackers often demand payment in cryptocurrency to obscure their identity. Funds paid as ransoms or obtained through such attacks may be laundered via gambling platforms, where they can appear as legitimate winnings. Accepting such funds can lead to regulatory scrutiny and damage to Goodfly N.V.'s credibility.

2.9 Sanctions and prohibited entities

Entities or individuals subject to international sanctions may use cryptocurrencies to circumvent financial restrictions. By transacting with these parties, gambling platforms risk severe legal consequences and reputational harm.

2.10 Scam coins

Scam coins are cryptocurrencies or tokens created with the intent to deceive investors or users. These coins may lack legitimate use cases and are often involved in pump-and-dump schemes or fraudulent ICOs.

2.11 Stolen coins

Cryptocurrencies obtained through theft, such as wallet hacking or exchange breaches, can be used on gambling platforms to obscure their origin. Accepting stolen coins could result in financial losses to Goodfly N.V. if assets are traced and seized.

2.12 Terrorism financing

Cryptocurrencies can be used to facilitate financial transactions for terrorist organizations due to their decentralized and pseudonymous nature. Gambling platforms might unintentionally process funds tied to these activities. Regulatory bodies impose strict penalties on platforms that fail to prevent such transactions, including potential license revocation.

2.13. Suspicious wallets and transactions

Certain wallets are flagged as suspicious due to their connections with illegal activities, high-risk jurisdictions, or irregular transaction patterns. Failing to monitor and block such wallets could result in fines, reputational damage, and regulatory action.

2.14 ICO and token sales

Funds raised through fraudulent ICOs or token sales may be laundered through gambling platforms, as they provide a mechanism for converting cryptocurrencies into perceived legitimate funds. Platforms must scrutinize tokens and cryptocurrencies associated with ICOs before accepting them.

3. Risk mitigation measures

To address the identified risks, Goodfly N.V. implements a comprehensive set of controls and procedures aimed at ensuring compliance, security, and operational integrity. These measures are designed to minimize exposure to illegal activities while maintaining a seamless experience for legitimate users.

3.1 Mandatory KYC (Know Your Customer) procedures

Every player intending to use cryptocurrency for transactions on Goodfly N.V.'s platforms must complete thorough identity verification. This includes submitting government-issued identification documents and undergoing cross-referencing against international sanctions lists, politically exposed persons (PEP) databases, and adverse media sources.

3.2 Transaction monitoring and screening

All cryptocurrency transactions are continuously monitored using advanced AML tools such as AMLBot. These tools analyze transaction histories, flag suspicious activity, and evaluate the risk level of wallets based on their association with illicit operations like dark markets, mixers, or scam coins. Alerts are automatically triggered for high-risk transactions, enabling the compliance team to block or freeze funds and conduct a deeper investigation when needed.

3.3 Approved cryptocurrency list

To prevent exposure to high-risk assets, the platform maintains a whitelist of approved cryptocurrencies. This list is developed based on strict criteria, including legal recognition in operational jurisdictions, a clean transactional history, and support from regulated exchanges. Privacy-focused coins, such as Monero, are explicitly prohibited due to their potential misuse for anonymous transactions. The company also ensures that scam coins and tokens linked to fraudulent ICOs or pump-and-dump schemes are excluded.

3.4 Collaboration with regulated exchanges

All transactions are routed through licensed and regulated cryptocurrency exchanges that enforce robust AML and KYC protocols. These exchanges are selected for their transparency, compliance with international standards, and ability to provide detailed transaction reporting. This measure ensures that the funds entering and leaving the platform originate from legitimate and verified sources.

3.5 Sanctions and jurisdictional restrictions

Goodfly N.V. enforces strict restrictions against users from jurisdictions or entities subject to international sanctions. IP addresses and payment sources linked to sanctioned countries are actively blocked. The list of restricted jurisdictions is reviewed and updated regularly to reflect changes in global regulatory frameworks and maintain compliance. The list is constantly updated using automatic monitoring tools.

3.6 Limits on anonymous transactions

To further reduce risks associated with anonymity, the platform enforces strict limits on transactions for unverified accounts, if any are permitted. High-value transactions or those originating from flagged wallets undergo manual review by the compliance team. This ensures that all substantial activity is scrutinized for legitimacy and compliance.

3.7 Regular compliance audits

Periodic compliance audits are conducted to ensure that all risk mitigation measures are effectively implemented. These audits include reviewing flagged transactions, assessing the effectiveness of AML tools, and verifying adherence to internal KYC procedures. The audits also identify areas for improvement, ensuring the policy remains adaptive to emerging threats and regulatory changes.

3.8 Employee training and awareness

Staff members involved in cryptocurrency-related operations receive regular training on AML/CFT compliance, risk identification, and the use of monitoring tools. This training ensures that employees are well-equipped to detect and respond to suspicious activities, strengthening the company's overall risk management framework.

3.9 Immediate reporting of suspicious activities

Suspicious transactions or activities are promptly reported to relevant authorities in compliance with local and international laws. This includes filing Suspicious Activity

Reports (SARs) and cooperating with law enforcement agencies during investigations.

3.10 Risk-based approach to player monitoring

The platform employs a risk-based monitoring approach, applying enhanced scrutiny to high-value players, accounts exhibiting unusual behavior, and those linked to high-risk jurisdictions. This allows the company to allocate resources efficiently while ensuring a robust defense against potential threats.

4. Monitoring and Policy Updates

Goodfly N.V. recognizes that the cryptocurrency landscape is dynamic, with new risks and regulatory changes emerging regularly. To maintain the effectiveness of this policy, a robust monitoring and updating framework has been established.

4.1 Continuous monitoring of transactions

The company employs state-of-the-art tools to continuously monitor cryptocurrency transactions on the platform. These tools analyze transaction patterns, evaluate wallet risk scores, and flag irregularities in real-time. Alerts triggered by suspicious activity are reviewed by the compliance team, and appropriate actions, such as freezing accounts or initiating investigations, are taken promptly.

Additionally, the platform maintains a feedback loop between transaction monitoring results and risk management protocols. Lessons learned from flagged cases are integrated into ongoing policy refinements to strengthen defenses against similar threats in the future.

4.2 Regular policy reviews

The cryptocurrency risk policy is reviewed quarterly or whenever significant changes occur in the regulatory or operational environment. These reviews ensure that the policy remains aligned with:

- Updates to international standards, such as FATF recommendations or EU AML directives.
- Jurisdiction-specific gambling and cryptocurrency laws in the markets where the company operates.
- Emerging threats and trends in the cryptocurrency ecosystem, such as the proliferation of new anonymizing tools or scam tokens.

The review process involves collaboration between the compliance team, legal advisors, and external auditors, ensuring a holistic and up-to-date approach to risk management.

4.3 Incident response and reporting

In the event of policy violations, flagged transactions, or regulatory breaches, an incident response protocol is activated. This includes:

- Isolating the affected accounts or transactions to prevent further activity.
- Conducting a root cause analysis to identify gaps in the monitoring framework.
- Reporting the incident to relevant authorities, including financial regulators and law enforcement, in compliance with applicable laws.

This actions must be taken by Goodfly N.V. within 5 business days.

The outcomes of these incidents are documented and analyzed to improve the policy, reduce vulnerabilities, and ensure transparency with stakeholders.

5. Accountability and roles

The successful implementation of this policy relies on clearly defined roles and responsibilities within the organization.

5.1 Compliance Officer

A dedicated Compliance Officer oversees the enforcement of the cryptocurrency risk policy. Their responsibilities include:

- Ensuring that all transactions are monitored and evaluated under the policy.
- Conducting regular compliance audits and maintaining documentation of findings.
- Acting as the primary point of contact for regulators and law enforcement agencies.

5.2 Employees

All employees involved in cryptocurrency-related operations are required to:

- Adhere to the guidelines outlined in this policy.
- Complete mandatory training programs on AML/CFT compliance and cryptocurrency risk management.
- Report any suspicious activity to the Compliance Officer without delay.

5.3 External Partners

Third-party service providers, such as payment processors and cryptocurrency exchanges, must align with the company's compliance standards. Contracts with these partners include clauses that:

- Require adherence to AML/CFT regulations and cooperation in investigations.
- Allow audits to ensure compliance with agreed-upon standards.