

CRYPTO USAGE RISK POLICY

Introduction

This document sets out the Green Forest Group N.V. (the “Company”) Crypto Use Policy, which meet the applicable laws, international standards, Financial Action Task Force (FATF) and Curacao regulations as the National Ordinance Containing Rules concerning Games of Chance (the “LOK”) and the relevant AML Policy aiming to reduce exposure from money laundering and terrorist financing, (the “Policy”).

The purpose of this policy is to provide a legal framework and guidance on trade with or use of crypto. It describes how the Company will implement the necessary steps to identify, assess, and control the risks arising from the use of crypto assets, given their potential to facilitate money laundering, terrorist financing, or other illicit actions.

This policy will be consistent with, and complementary with the AML/CFT Risk Assessment Policies and Procedures (the “AML/ CFT Policy”) that are already in place internally at the Company as part of its collective risk-based compliance framework.

Scope

This Policy shall apply to all of the Company’s businesses, units, employees, systems and third parties involved in any way in the carrying out of functions or provision of services related to operations with cryptocurrencies on behalf of the Company.

In particular, this Policy has established internal controls and due diligence procedures regarding:

- Compliance with all AML/CFT requirements applicable in the country of Curacao, including the National Ordinance on Identification of Clients (NOIS), the National Ordinance on Reporting Unusual Transactions (NORUT), the LOK and as well the international standards set by FATF.
- Review and monitor all crypto transactions such as deposits and internal transfers based on a risk-based approach. Withdrawals will be completed using the same previously verified payment methods that the customer utilized as part of the Closed Loop strategy of the Company.
- Detect, report, and raise alerts on any cryptocurrency-related suspicious activity to the relevant authorities where necessary, including but not limited to the Financial Intelligence Unit (FIU);
- Transparency, trackability, and auditability in each cryptocurrency transaction performed on the platform or through the Company.

- Reduce the risk associated with crypto assets in anonymous transactions, high-risk territories and unregulated virtual asset service providers (VASPs)

The Company will review this Policy and may update it from time to time in accordance with changes to applicable laws and regulations, regulatory expectations, technological change and best industry practice.

Definitions

For purposes of this policy, the terms below shall have the meanings specified:

- Virtual Asset (VA): representation of value existing only in digital format that may be traded or transferred electronically and used either for investment purposes or as a means of payment.
- Cryptocurrency: type of virtual asset using primarily cryptographic techniques to secure transactions and control the creation of new units.
- FIAT: currencies that are issued and backed by a government or central bank.
- Virtual Asset Service Provider (VASP): it stands for any natural person or legal entity carrying out one or more of the following activities as a business:
 - ✓ Exchange between virtual assets and fiat currencies.
 - ✓ Exchange between one form of virtual asset to another form thereof.
 - ✓ Transfer of virtual assets.
 - ✓ Storage and/or management control which requires a proprietary key for access, taking virtual assets into custody through participation in an issuer's offer and/or sale of virtual asset derivatives.
- Wallet: Digital tool or software storing private and public keys which interfaces with different blockchains so that users can send or receive virtual assets from each other. All the wallets use must be properly verified by the Company or its crypto payment service provider
- Mixers or Tumblers: service or technology which hide the origin or destination of crypto assets through mix up together funds from many users. Useful for anonymizing transactions which used is forbidden under this policy.
- Sanctioned Jurisdictions: territories currently subject to international financial sanctions, trade restrictions or any other limitations that are in force as determined in Curacao laws, FATEF, the United Nations, the Office of Foreign Assets Control or the EU regulations.

- **High-Level Risk Jurisdiction:** a country that has strategic AML/CFT deficiencies and which deserves reinforced vigilance prescribed by an authoritative body like the FATF or the FIU in Curacao.
- **Source of Funds (SOF):** it refers to the origin of funds for a particular transaction or series of transactions.
- **Source of Wealth (SOW):** the origin of an individual's total wealth, i.e., how a person came to have the overall funds or assets that he or she holds.

General principles

The Company applies a risk-based approach to all crypto related activities. Company recognises the risks associated with gaming operations especially when enabling the use of cryptocurrencies; therefore, when creating and implementing this Policy, it is necessary to adhere to the following principles:

- Any crypto transaction must be recorded and traceable
- The system will generate a comprehensive logging to support internal and external audits.
- Risk-based controls are applied according to customer profiles and transaction patterns.
- The use of Mixers or Tumblers are strictly prohibited.
- Only regulated VASPs that operate in a non-sanctioned or high-risk jurisdiction are allowed.
- Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency and they can't be sold, bought or exchanged .
- The withdrawals are allowed in cryptocurrency only to wallets that have been verified and match the customer's verified profile subject to the Company's application of the closed loop principle.

Risky factors

The Company adopts a risk-based approach to any crypto related activities. This means that, when VAs are being used, the Company identifies risk by category as follows:

- i. Anonymity and traceability of cryptocurrencies.
- ii. Exposure to high-risk jurisdictions or sanctioned countries.
- iii. Potential use of an unregulated VASP

- iv. Client risk profiles that are inconsistent with declared Source of Funds or Source of Wealth.
- v. Use of technological tools, such as Mixers or Tumblers, to bypass payment controls during the crypto transaction.
- vi. The speed and irreversibility of crypto transactions that obstacle to traditional AML risk analysis
- vii. Risks arising from distribution channels, such as third-party interfaces, where the Company does not have full control.

It is important to note that, the existence of a single risk does not necessarily mean that a criminal activity is taking place; however, the presence of multiple risks with no logical business explanation raise the suspicion of a potential criminal activity. In accordance with to AML/CFT Policy, the Company examines these risks and reduces them with the mitigation measures in the sections below.

Risk mitigation measures

Ongoing monitoring: The company will maintain ongoing monitoring of all cryptocurrencies in operation to find unusual or suspicious activity, as stated in Section 7.1 of the AML/CFT Policy.

AML policies: The SoF and SoW crypto deposits are assessed to verify the origin of money and ensure consistency with the player's profile.

Wallet ownership verification: The customers may use only the wallet that it is registered on their name.

Geolocation Controls: The Company use technological tools of geolocation and IP analysis to detect access from sanctioned or risky jurisdictions.

Thresholds and Triggers: Enhanced Due Diligence (EDD) is applied when crypto transactions breach defined thresholds or exhibit red flag warnings as defined by FATF.

Reliance on third parties to perform Customer Due Diligence (CDD): The third party should be subject to CDD and record-keeping requirements of the Company.

Withdrawals: Withdrawals will be made specifically using confirmed payment methodologies previously utilized by the customer, in compliance with the Company's Closed Loop Policy.

VASPs EDD: The VASPs are subject to enhanced due diligence, including verification of their regulatory status, licensing jurisdiction, compliance controls and reputation.

VAs review: The Company shall, in compliance with the article 4.2.1 of the LOK regularly review the risk assessment for using VA.

Cryptocurrencies transactions: The cryptocurrencies transactions including deposits and withdrawals, are processed through the Company's approved crypto payment service provider and where technically feasible, the withdrawal shall be made to the same wallet used for the deposit. Any deviation from this policy must be subject to enhanced due diligence and compliance approval

Prohibited activities

Under the Policy the following activities are strictly prohibited:

- Anonymous cryptocurrencies that hide transaction traceability
- Mixers, tumblers or similar technologies.
- Third-party wallets or wallets not KYC-verified.
- Deposits or withdrawals involving sanctioned jurisdictions or unregulated VASPs.
- Transactions inconsistent with the customer's declared profile, SoF or SoW.

Unusual crypto-related transactions.

The following types of crypto-related transactions, actual or intended, may be considered unusual and require reporting:

- Transactions involving NAf. 5,000 or more (or its crypto equivalent) per gaming day, whether in a single transaction or aggregated amount.
- Cashless transactions or withdrawals executed via cryptocurrency and then converted to fiat currency.
- Transactions executed on behalf of, or involving, persons or entities listed under international sanctions.
- Presumed money laundering or terrorist financing transactions.

For the avoidance of doubt, the Company and any of its officers, directors, or employees are protected from criminal and/or civil liability arising out of disclosure when in earnest submission in good faith to FIU.

Record keeping

All crypto transactions and related due diligence documentation will be kept by the Company over a minimum of five years after ending a business relationship, in accordance with the AML/CFT Policy and the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction.

Reporting

The Money Laundering Reporting Officer (MLRO)/Compliance Officer designated by the Company is in charge of the reporting with the competent authority any circumstances for which the Company has not received sufficient verifying information or suspect of transactions or other actions i) involve funds derived from illegal activities, (ii) are intended to conceal funds from illegal activities, or (iii) involve the use of the Company system to facilitate criminal activity, may give rise to its report to the FIU in Curacao.

Based on article 11 of the NORUT and the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, the Company will report any unusual or intended unusual transactions to the FIU without delay. To support this obligation, the Company has set out clearly internal procedures including:

- Recognizing unusual transactions.
- Any transaction inconsistent with the customer's profile, involving unusually large amounts or complex structures.
- Standardizing the documentation of all unusual transactions, including identification documents, transaction records and internal assessments, so as to keep them in a format that management approves.
- Internal reporting to the Compliance Officer, who shall maintain a secure filing system, and determine whether escalation to FIU is required, also must be in place.
- In cases where a reported transaction is not ultimately submitted to the FIU, the Compliance Officer and/or management will document and sign off the reasons for this non-submission.
- All unusual individual transactions or series of transactions shall be reported internally to the Compliance Officer, without delay, together with all supporting material of documentation.

The Compliance Officer is responsible for submitting reports via goAML in English to FIU appropriately. If eligible, the Company may request bulk reporting access through its FIU-appointed account manager.

Roles and responsibilities

- Ensuring that the policy is implemented and enforced.
- Training and direction regarding crypto risk-related risks.
- Ultra-high-value-transaction flagged transactions and pulling STR when needed.
- Properly fortifying the architecture of systems to monitor and control crypto transactions.

The Policy is also adhered to by all employees, contractors and suppliers involved in crypto-related operations. The Compliance Officer under the oversight designed MLRO, is responsible for:

- Ensuring the Policy is properly implemented and enforced.
- Providing training and guidance on crypto-related AML/CFT risks.
- Reviewing high-risks or unusual crypto-related transactions.
- Reinforcing the system used to monitor and control for cryptocurrencies transactions
-

Training and awareness

Any of the Company employees should be trained regarding this Policy and AML/CFT risk on crypto-related transactions. The Company shall further conduct ongoing campaigns to educate on emerging threats, warning signs and best practices for managing crypto risks.

Policy review

The Company shall review this Policy an annual basis minimum or when there is any change in the applicable regulatory framework or our internal risk profile. All modifications require the signature from the Compliance Officer