.

AML/CFT & KYC Policy

Issuer: VANIR VENTURES B.V.

Version: 2.1

Date: 22/04/2026

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this policy is to set out VANIR VENTURES B.V. (hereinafter "Vanir" and/or the “Company”) internal practice, measures, procedures and controls relevant to the prevention of Money Laundering (ML) and Terrorist Financing (TF) and further assist Vanir to achieve the following objectives:

- Implement and comply with all legal and regulatory requirements that govern its operations.
- Ensure adequate processes are implemented in order to establish the identity of any customer it engages with, coupled with the monitoring of transactions made by such customers so as to identify risks;
- Enable the tracking and identification of suspicious transactions/activities as well as to prevent possible fraud with regards to risks to its financial strength and/or reputation.
- To report any suspicious transactions/activities in relation to money laundering, terrorist financing or proliferation financing, both internally and externally to the appropriate authorities; and
- Maintain its integrity, credibility and reputation;

Vanir Ventures B.V (“Vanir”) strives to maintain an effective anti-money laundering and combating terrorist financing (“AML/CFT”) program, Vanir employs the Know Your Customer (“KYC”) policy and procedure.

KYC is used to assess indicators of perceived money laundering risk at the Customer level. This is accomplished by establishing various risk indicators and identifying Customers who behave in the outlier ranges of these indicators. This KYC process enables Vanir to adequately identify higher risk Customers and to take appropriate action to mitigate the risks.

KYC policies are fundamental to an AML/CFT program. From Vanir’s perspective, knowing whom we do business with is crucial in preventing instances of inadvertently facilitating money laundering and/or other crimes. An inadequate Know Your Customer system can result in Vanir as a limited entity, as well as individual employees, being subject to civil and/or criminal penalties. Such penalties can vary from one country to the other.

The Company operates under a licence issued in Curaçao and is subject to the National Ordinance on Games of Chance (Landsverordening op de Kansspelen – LOK, P.B. 2024, no. 157), as well as all applicable Curaçao AML/CFT legislation and regulatory requirements issued by the Curaçao Gaming Authority (CGA), which acts as the licensing and supervisory authority for the Company’s gaming operations and AML/CFT compliance.

The Company complies with the following Curaçao legal and regulatory framework:

- National Ordinance on Games of Chance (LOK);

- National Ordinance on the Reporting of Unusual Transactions (NORUT);

- National Ordinance on Identification when Rendering Services (NOIS);

- Sanctions Ordinance;

- Criminal Code of Curaçao; and

- Applicable guidance, directives and requirements issued by the Curaçao Gaming Authority (CGA).

The Company provides remote online gaming services on a cross-border basis, limited to permitted jurisdictions in accordance with its geographical risk assessment and market restrictions. In managing cross-border ML/TF risks, the Company applies a risk-based approach aligned with international standards, including FATF Recommendations and relevant EU AML/CFT best practices, where appropriate.

The AML/CFT framework implemented by the Company is based on its Business-Wide Risk Assessment (BWRA), which identifies risks associated with its products, customers, delivery channels and geographical exposure. The controls, procedures and monitoring measures described in this Policy are designed to mitigate those identified risks within the Company's defined risk appetite.The KYC program includes:

- Risk-based requirements for Customers dependent on Customer's risk category arising from customer due diligence and enhanced due diligence reports CDD/EDD respectively);
- Measures to identify Sanctioned individuals and PEPs and take appropriate action;
- Ongoing monitoring of Customers and their transactions and reporting suspicious transactions as required;
- Keeping Customer Due Diligence information up to date; and
- Training and guidance for employees on AML/CTF issues
- Vanir is required to obtain information to identify Customers, to verify the Customers' identity
- information, to obtain information on the purpose and intended nature of the business relationship and to monitor such business relationships on an ongoing basis. Vanir is also required:
- to be satisfied that the Customers are who they say they are;
- to determine whether Customers are acting on behalf of others; and
- to understand the circumstances of Customers in order to protect Vanir from being used for fraud, ML/FT or any other criminal activity;

1.3 Scope

This procedure is applicable to all Vanir Customers. Departments, mainly the AML and RFP Departments employ this procedure under the oversight of the MLRO.

The implementation of the procedure requires adherence to Vanir's mission statement which reads as follows:

1.3.1 Employee's mission

- Strict adherence to the provisions of this Policy.

-Identification and examination of unusual transactions.

-Identify, assess and manage risks; and

-Stay informed of group, internal and local guidelines; and

-Maintain proper record keeping.

1.3.2 Vanir`s Mission:

-To have mechanisms in place which can monitor and report transactions, as required, when they happen.

-To establish criteria and develop clear acceptance policies and procedures for new and existing customers.

- To have mechanisms in place to be able to prevent and identify suspicious transactions when they take place; and

- To identify its risk areas and ensure that adequate controls are in place to mitigate against such risks.

1.3.3 Annual Review & Records Retention

This document is owned by the MLRO and is reviewed and updated annually or when there are significant changes to the policy/procedure.

The Company shall maintain AML/CFT records and provide compliance information and periodic reporting to the Curaçao Gaming Authority as required under applicable licensing and supervisory obligations. The Company shall cooperate with regulatory inspections, supervisory requests, and compliance audits.

The Company maintains an annual AML audit plan to assess the effectiveness of its AML/CFT framework, including customer due diligence, transaction monitoring, reporting obligations and internal controls. The audit is conducted periodically and includes both internal reviews and, where appropriate, independent external assessments. Findings are documented, reported to senior management, and remediation actions are tracked to completion.

Records of this procedure are stored in line with the Company's Retention Policy.

1.4 Money Laundering and Terrorist Financing

1.4.1 What is Money Laundering?

ML involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. Simply put, ML is the process of making dirty money look clean.

According to FATF, crimes such as illegal arms sales, narcotics trafficking, smuggling and other activities of organized crime can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits, creating the incentive to "legitimize" the ill-gotten gains through ML. When criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such illegal profits.

1.4.2 Stages of the ML process:

A. Placement:

Placement is considered to be the first stage in the ML process, whereby funds (usually cash) generated from criminal activities are placed into the financial system (such as banks, casinos or other non-financial organizations) and smuggled within or outside the country in order to conceal their source and avoid their detection by authorities. This can be achieved through: smuggling cash, transfers and shadow companies among others.

B. Layering:

The second stage of ML is about the disassociating of the funds from their illegitimate source through creating complex layers of financial transactions designed to conceal the ownership of funds and any audit trail in order to hide the original source of funds and ensure anonymity. The purpose of layering is not only to disguise the funds illegal source but also move the money to a place where they will not attract any attention.

C. Integration:

Integration is the final stage in the process. It is this stage at which the money is assimilated with legitimate financial assets. Integration achieves the primary objective of ML by making these funds appear to have been legally earned through, for example, international real-estate trading, trading of cars or diamonds and precious stones, and stock market capital gains among others. Therefore, at this stage illegally obtained funds is put back into the real economy, as legal and clean money.

All employees are required to know the three stages of the ML process (placement, layering and integration) and to be able to distinguish, uncover and disrupt them, This emphasizes the importance of realizing and understanding its stages in order to adhere to objectives of the mission.

1.4.3 What is terrorist financing?

TF includes the provision, gathering, or procurement of funds by any means, whether directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part for the commission of terrorist acts or to finance terrorist acts. TF acts are defined as individual or collective acts of violence, regardless of its motives, purposes or means, aimed at disturbing public order or endangering public safety and security or jeopardize human lives.

1.4.4 What is Proliferation financing?

Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development or for the export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes). It involves the financing of trade in proliferation sensitive goods but could also include other financial support to individuals or entities engaged in proliferation.

1. 5 Differences between ML/TF

The primary objective of TF is to intimidate a population to compel a government to do or abstain from doing an act. Terrorism is a crime of purpose, based on ideological beliefs, usually for publicity and political purpose. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. TF's primary purpose is to disguise the ultimate use of the funds, as opposed to their origin. It can involve relatively small sums of money, which can have a huge impact in terms of death, destruction and disruption. Although terrorists may finance their activities through crime, legitimate funds can also be misappropriated to finance terrorism.

On the other hand, the primary objective of ML is the financial gain and the fact that the funds used are originated from illegal activities.

Money laundering	Terrorist financing
✓ **Source**, money earned from crime	✓ **Source**, legal & illegal funds
✓ **Concealment** of source	✓ **Aim** to to collect money to carry out subversive activities Concealment of destination
✓ **Legalise** earning from crime	✓ Use of Money for activities to harm society
✓ **Aim/Motivation** is PROFIT	✓ Motivation is idealogical beliefs
✓ Money laundered remains/**comes back to the owner (circular process)**	✓ Money is spent and **does not remain** with original contributor of funds (linear process)

2. Business-Wide Risk Assessment (BWRA)

The Company conducts and maintains a documented Business-Wide Risk Assessment (BWRA), which identifies and evaluates the money laundering, terrorist financing and proliferation financing risks to which the business is exposed.

The BWRA considers, at a minimum:

- Customer risk, including behaviour, transaction patterns, and profile;

- Product and service risk, including the nature of online gambling products offered;

- Delivery channel risk, arising from non-face-to-face onboarding and remote payment methods;

- Geographical risk, including customer location and payment flows; and

- Regulatory and operational risks associated with multi-licence operations.

The assessment identifies potential misuse scenarios, including rapid deposit and withdrawal cycles, use of third-party funds, multi-accounting, and recycling of gambling proceeds across operators.

Mitigation measures include closed-loop payment controls, automated transaction monitoring, risk-based CDD and EDD, and ongoing behavioural analysis.

Residual risk is assessed after the application of controls, and is currently determined to be Low–Medium, reflecting the Company's EEA-focused customer base, regulated payment methods, and effective AML controls.

The BWRA is reviewed at least annually, or sooner where there are material changes to the business model, products, delivery channels, or regulatory environment. The BWRA is approved by senior management.

2.1 Technological and Product Risk Assessment

The Company performs a risk assessment prior to the introduction of any new products, services, delivery channels, payment methods, or technologies.

This assessment evaluates the potential money laundering, terrorist financing, and proliferation financing risks associated with such developments, including risks arising from non-face-to-face interactions, automation, or new payment mechanisms.

The assessment considers whether existing AML/CFT controls are sufficient to mitigate identified risks and determines whether additional controls, monitoring rules, or due diligence measures are required prior to implementation.

New products or technologies are not deployed until the identified risks are adequately assessed and mitigated in line with the Company's risk appetite.

2.2 Monitoring the Effectiveness of AML/CFT Controls

The Company continuously monitors the effectiveness of its AML/CFT framework to ensure that identified risks are adequately mitigated.

This includes the ongoing review of transaction monitoring rules, alert generation, and escalation processes to assess whether they appropriately identify unusual or suspicious activity.

The Company evaluates the effectiveness of its controls through:

- periodic internal reviews of transaction monitoring alerts and outcomes;
- analysis of unusual transaction reports and reporting patterns;
- findings from internal and external AML audits; and
- feedback from regulatory inspections or supervisory interactions.

Where weaknesses or inefficiencies are identified, the Company implements corrective actions, including adjusting monitoring thresholds, enhancing due diligence procedures, or strengthening internal controls.

All identified deficiencies and remediation actions are documented and tracked to completion.

3. AML/CFT & KYC Policy

3.1 Initial Customer Registration

Customers who sign to any of the brands owned by Vanir Ventures B.V. are first required to provide personal information listed in the Customer Acceptance Policy.

3.1.1 Preventing Underage Gaming

Vanir Ventures B.V. works to prevent underage individuals from having access to its services. This is done by not allowing anyone under the age of 18 to sign up for an account with Vanir Ventures B.V. As part of Verification, which is described in the Customer acceptance policy, customers need to confirm that they are over 18 to proceed with account registration. Furthermore, third-party databases are available for further checks to be conducted. If the information cannot be confirmed by the third-party databases, Customer Due Diligence processes would be triggered to further make sure the individual signing up for Vanir services is in fact of legal gaming age. Any customers identified as underage will not be allowed to use any of our services.

3.2 Customer Risk Assessment

The cornerstone of the risk-based approach is the risk assessment which allows Vanir Ventures B.V. to identify the risks it is exposed to. On this basis, Vanir Ventures B.V. is able to draw up, adopt and implement measures, policies, controls and procedures that address any identified risks.

While most Customers adopt low risk funding mechanisms, transact at relatively low amounts, originate from low risk jurisdictions and in turn pose considerably lower risk – Vanir carries out a full risk assessment for players.

The detailed scoring methodology is maintained in the Company's internal Customer Risk Assessment framework.

3.3 KYC Thresholds

3.3.1 Verification

Upon initiating their first deposit, the Customer is also screened against politically exposed persons ("PEP") and Sanction lists as well as a risk assessment is generated.

PEP screening is repeated within 30 days of a customer reaching the applicable deposit threshold, even where prior screening has been completed.

Customer due diligence ("CDD") is applied at onboarding and, at the latest, upon reaching a cumulative deposit threshold of €2,000 or earlier where risk indicators arise.

3.3.2 Customer Due Diligence ("CDD")

CDD requires the application of the following measures:

- Identification of the customer and verification of the same using documents, data or information obtained from reliable and independent sources.
- Conducting ongoing monitoring of transactions undertaken by Customers to ensure that they are consistent with Vanir's knowledge of the Customer (including source of funds).
- Application of identification procedures and due diligence measures, at appropriate times, for both new and existing Customers.

In relation to Vanir's assessment of risk, we consider:

(a) Customer Risk, including the customer profile, geographic location, transaction volumes, frequency of play and behaviour;

(b) Transaction Risk, focusing on the size, volume and complexity of transactions and patterns of gambling activity;

(c) Product/Service Risk, associated with the online gambling products offered; and

(d) Delivery Channel Risk, arising from the non-face-to-face nature of the business relationship and remote payment methods used.

Based on these factors, customers are assigned a low, medium or high-risk rating. Standard CDD is applied to customers assessed as low or medium risk. Customers may be requested to provide documentation confirming their identity, address and ownership of payment methods (where applicable). Vanir may also request additional verification measures, such as a selfie holding an identity document, where deemed necessary.

The events that trigger the CDD procedure are as follows:

- When a Customer registers.

- When a Customer reaches the cumulative threshold of 2,000 euros or more.
- When a Customer requires to withdraw to a method which is not the same as the one they used to deposit (because the method does not support it)

3.3.2.1 Verifying Identity

A copy of an identity document must include the player's full name, date of birth and expiration date. The document provided must contain evidence of its legal validity.

3.3.2.2 Acceptable documents for Identity

These include photo ID documents such as passports, ID cards and/or Driving Licenses. An extensive list of acceptable documents can be found in Appendix A of this document.

3.3.2.3 Acceptable documents for Address Verification

Unless the ID can also serve the purpose of POA, address verification generally includes government issued documents (e.g. utility bills) or bank issued statements not older than 90 days. An extensive list of acceptable documents can be found in Appendix A of this document.

3.3.2.4 Verification of Customer's Payment Method

A payment method document must include the Customer's full name, information to identify a specific payment method and in case of card payments – card expiration date. The following documents are accepted:

- Payment card – must include the Customer's name, card number, and expiration date. Both sides of the card must be provided, sensitive data may be obfuscated (e.g. middle digits of card number and security code)
- Bank account – must include the player's name, full IBAN number, issuing institution's name, logo and date of issuance. The document can be provided as a copy or a screenshot of a bank statement (where applicable).

E-wallet – must include the player's name, account number/name and the transfer to Vanir. The document can be provided as a screenshot from the e-wallet account.

3.3.3 Enhanced Due Diligence ("EDD")

Where the risks of money laundering or terrorist financing are higher, the Customer will be classified as high risk and Vanir will conduct enhanced Customer due diligence ("EDD") measures, consistent with the risks identified. Enhanced due diligence is applied to Customers who are assessed as high risk based on the initial and/or the ongoing risk assessment. EDD is an additional measure to CDD, which includes an enquiry on the Customer's source of funds and/or wealth that was used to make deposits to Vanir, as well as reviewing supporting documentation to the answers.

The criteria which constitute a high-risk customer may be found in the Customer Risk Assessment Policy. Vanir applies EDD measures to its Customers:

1. When dealing with natural persons from third countries identified by the FATF as high risk third countries and monitored jurisdictions;

2. In the cases of transactions or relationships with PEPs, their close family members and persons known to be close associates of PEPs,

3. In cases whereat there is high volume and size of transactions.

4. In other cases of higher risk that are identified by the company

In the event that a customer is identified as a Politically Exposed Person (PEP), the establishment or continuation of the business relationship is subject to approval by the MLRO and, where applicable, senior management.

In such cases, enhanced due diligence measures shall be applied, including the mandatory establishment and verification of the customer's source of wealth (SOW) and source of funds (SOF).

PEP customers are subject to enhanced and ongoing monitoring throughout the duration of the business relationship.

Vanir applies EDD measures in the above situations in order to manage and mitigate those risks appropriately. Vanir will always strive to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions and all unusual patterns of transactions, which have no apparent reasonable economic of lawful purposes.

3.3.3.1 Verifying the Source of Funds

Documents on the source of funds are requested from the Customers and must be provided in electronic form. Vanir can also recur to third party companies such as GB Group to gather or verify information concerning EDD. The Company assesses the plausibility of the customer's source of funds by comparing declared income, occupation, and available financial information against transaction behaviour and net deposits.

3.3.3.2 Acceptable documents for Source of Funds Verification

These generally include bank statements where the Customer name and account balance are visible, along with pay slips and/or other income information. In case of businesses, typically the latest audited financial statements would need to be provided. An extensive list of acceptable documents can be found in Appendix B of this document.

3.3.3.3 Further EDD Reviews

If a high-risk Customer is allowed to continue using Vanir services, further EDD reviews may take place. Below is a non-exhaustive list of enhanced measures that may be taken to mitigate the risk in cases of high-risk relationships:

- more frequent updating identity of the Customer;
- obtaining the approval of senior management/MLRO to enter into or maintain the business relationship;
- increased and more frequent monitoring of transactions;
- gathering additional documents, data or information; or taking additional steps to verify the documents obtained;
- establishing transaction limits customized to the nature, scale and complexity of the Customer;
- increasing internal controls of high-risk business relationships;
- obtaining the approval of senior management/MLRO at the transaction level for products and services that are new for that Customer;
- obtaining regular credit reports or additional documentation;

3.3.4 Risk Based Approach

The Company adopts a moderate risk appetite aligned with remote gambling operations, accepting only risks that can be effectively mitigated through AML controls, monitoring, and EDD.

In money laundering and terrorist financing, a risk-based approach covers the following:

- the risk assessment of Customer relationships and business activities;
- the risk mitigation to implement controls to handle identified risks;
- keeping Customer identification and business relationship information up to date; and
- the ongoing monitoring of Customers and transactions.

Existing regulatory obligations, such as for Customer identification, are a minimum baseline requirement. Where enhanced due diligence is appropriate, a principle of the risk-based approach is to focus resources where they are most needed to manage risks within our tolerance level.

In addition to the above, the Company applies a structured customer risk assessment at onboarding and throughout the business relationship. Each Customer is assigned a risk level (Low, Medium, or High) based on a combination of risk factors.

The assessment considers, at a minimum:

- Customer profile, including occupation and source of income;

- Geographical risk, including country of residence and any exposure to high-risk jurisdictions;

- Transaction behaviour, including deposit amounts, frequency, and payment methods used;

- Product risk, based on the nature of the services used; and

- Delivery channel risk associated with non-face-to-face onboarding.

The assigned risk level determines the level of due diligence applied, including whether standard CDD or Enhanced Due Diligence (EDD) measures are required. The risk profile is reviewed and updated on an ongoing basis, particularly where changes in customer behaviour or activity are identified.

3.3.4.1 Ongoing Monitoring

Customers who have successfully undergone the CDD procedure that was initiated by the 2K threshold or where such measures were triggered at an earlier stage are monitored regularly.

All Customers who have undergone the CDD procedure are required to submit new documentation if there are significant changes spotted on the player's account.

In addition to automated transaction monitoring rules, all alerts generated by the system are subject to review by the Risk, Fraud and Payments Department (RFP).

Alerts are analysed to determine whether the activity is consistent with the customer's known profile, source of funds, and expected behaviour.

Where an alert cannot be reasonably explained or gives rise to suspicion, the case is escalated to the MLRO for further assessment.

The MLRO reviews the case, including transaction history, customer profile, and any supporting documentation, and determines whether the activity is suspicious and requires reporting to FIU Curaçao.

All alert reviews, decisions, and escalation outcomes are documented and retained in accordance with the Company's record-keeping requirements.

3.4. Client Acceptance Policy:

- The Client Acceptance Policy(hereby referred to as the "CAP") defines the criteria for Vanir's acceptance of new Customers and defines the categorization criteria followed by Vanir. The MLRO is responsible for monitoring and providing advice and guidance where necessary for the implementation of all the provisions of the CAP which shall be signed off by the Management of Vanir.

- The CAP is based on the following principles:

1. Vanir should only do business with those customers of good integrity and reputation, who are involved in legitimate business activities and whose wealth and funds are derived from legitimate sources.

2. From the information gathered, Vanir should be able to obtain a reasonable understanding of its Customers and be alert to unusual and suspicious activity as well as activity that is inconsistent with the expected.

4. Document Checking Procedure

All steps outlined below are performed by the Risk, Fraud and Payments Department ("RFP"), unless otherwise stated:

1. Agents review the document provided by the Customer to ensure that the document is visible in its entirety and that all details are clear.

a. If the document is an ID, the document has to be valid (expiration date has not passed), all the numbers and photographs must be visible and the document must be on the list of acceptable ID documents outlined in Appendix A

i. Agents also look to ensure that the document does not appear to be altered in any way and that it fits the expected ID format.

b. If the document is a bank statement, the document needs to be visible in its entirety, the name of the Customer needs to be visible (on at least one page if it is a multi-page document) and it must be on the list of acceptable documents listed in Appendix A. In case of Source of Funds documents are listed in Appendix B.

i. The details that can be obfuscated from the documents are ones that are not pertinent to the check being performed (e.g. full credit card/CVV numbers)

c. All other provided documents must be clearly visible and must display the name of the Customer on at least one of the pages.

i. Again, only details that can be obfuscated from the documents are ones that are not pertinent to the check being performed (e.g. full credit card/CVV numbers)

2. If the document does not meet one of the requirements outlined in step 1, the agent rejects the document, informs the Customer on the reason behind the rejection and requests a valid copy of the document.

a. If the Customer is not able to provide an acceptable copy of the requested document within 30 days, the business relationship is terminated. Within those 30 days, all withdrawals are withheld.

b. If the Customer is unable to provide the requested information and his or her actions appear suspicious and or indicative of Money Laundering, Terrorist Financing and/or Fraud (some indicators are listed in Appendix C) – the Customer's profile and all information collected to that point is forwarded to the MLRO for further review.

i. If the activity is confirmed to be suspicious by the AML staff, the Customer profile is blocked, limited or suspended and relevant Suspicious Activity Reports are filed.

ii. The Customer is not informed of these suspicions and subsequent actions, and the necessary action is taken by the MLRO where applicable, such as raising an STR. The Company strictly prohibits tipping-off in accordance with Curaçao AML legislation.

3. If the uploaded documents meet the requirements outlined in Step 1 – the agent takes one of the following actions:

a. If only the verification of Identity was required – upon their verification the agent may proceed in verifying the account

b. If the checking of source of funds was necessary or there is a need for EDD, upon collecting all the required EDD documents the agent forwards them to the Deputy MLRO/MLRO for additional checking:

i. The Customer transaction history with Vanir is then reviewed, along with the provided documents and explanations and evaluates if any further information is necessary.

ii. If further information is required, the Customer is contacted to provide the necessary information.

iii. Once the MLRO is satisfied with the provided documentation, the analyst will be informed to verify the account.

4. If the Customer is unable or refuses to provide any of the requested documents, his or her account cannot be verified, and she/he would not be allowed to continue using Vanir services.

a. If the Customer's refusal to provide documentation appears suspicious and/or indicative of Money Laundering, Terrorist Financing and/or Fraud – the Customer's profile and all information collected to that point is forwarded to the MLRO for further review and a potential filing of a Suspicious Transaction Report.

4.1 Personal Information Collected at Registration:

- Full legal name
- Full residential address
- Date of birth
- Email address
- Telephone number

4.2 Suspicious Activity Reporting – Unusual Transactions

Employees are required to promptly report any knowledge, suspicion, or reasonable grounds to suspect money laundering, terrorist financing, fraud, or other criminal activity to the MLRO in accordance with Curaçao AML/CFT legislation and the Company's internal reporting procedures.

Internal reports must include all relevant information known to the employee, including customer identifiers, transaction details, behaviour observed, and reasons for suspicion. Timely and accurate reporting is essential to enable appropriate assessment and, where necessary, external reporting.

Failure to report suspicions in accordance with this Policy and applicable Curaçao AML/CFT obligations may result in disciplinary action and may expose the Company and individuals to regulatory or legal consequences.
Internal unusual activity reports shall be submitted to the MLRO via:
Christos@vanirventures.com

Reporters are not routinely provided with feedback on the outcome of their internal reports due to confidentiality requirements.

Where suspicion is confirmed, the MLRO will submit an Unusual Transaction Report (UTR) to the Financial Intelligence Unit Curaçao (FIU Curaçao) via the goAML reporting system in accordance with applicable Curaçao AML/CFT obligations.

Where a decision is made not to submit a UTR, the rationale for such decision is documented, including the analysis performed, supporting evidence reviewed, and justification for concluding that the activity does not give rise to suspicion.

Failure to comply with this Policy and applicable AML/CFT obligations may result in disciplinary action, up to and including termination of employment.

In addition, non-compliance may expose the Company and the individual to regulatory sanctions, financial penalties, and potential criminal liability under applicable Curaçao legislation.

Breaches of AML/CFT obligations may also result in significant reputational damage and may impact the Company's ability to maintain its licence and continue operations.

4.3 Legal and Regulatory Framework

Vanir Ventures B.V. reports unusual transactions in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and related AML/CFT legislation of Curaçao.

All unusual or suspicious activities identified in relation to customers, transactions, or attempted transactions are reported to FIU Curaçao via the goAML reporting system.

Unusual transaction reporting obligations apply irrespective of transaction amount and include attempted, incomplete, or declined transactions.

UTRs must be submitted promptly after suspicion is formed and without undue delay.

UTR records, internal reports, and supporting documentation are retained for a minimum of five (5) years in accordance with Curaçao AML/CFT record-keeping requirements.

4.4 Record-Keeping Requirements

Vanir Ventures shall maintain all AML/CFT-related records for a minimum of five (5) years after:

- the business relationship has ended; or
- the date of the last transaction, whichever is later.

The following records must be retained:

- Customer Identification Records (KYC)
- POI, POA, payment method verification
- EDD documents, SoF/SoW
- PEP and sanctions screening results
- Risk-assessment
- Transaction Records
- Full deposit/withdrawal history
- Failed and declined transactions
- Internal AML Records
- Internal unusual activity reports
- Case notes, internal investigations, escalation logs
- Transaction monitoring alerts and outcomes
- AML analyst review notes
- External AML Reporting
- UTR submissions to FIU Curaçao
- FIU correspondence, requests, feedback
- Audit trails related to UTR filings
- Technical Logs
- System access logs for AML-relevant data

4.4.1 Security & Accessibility of Records

- Records must be securely stored, protected from alteration or deletion.
- Only AML staff, MLRO, and authorised personnel may access them.
- Records must be readily retrievable within 24–48 hours upon request by CGA or FIU Curaçao.

5. Appendix

5.1 Appendix A - Acceptable Documents for Identity Verification

Proof of Identity

It must be a legal government-issued document, containing a facial image of the owner, both sides of the document need to be provided and documents that are past the expiration date will not be accepted.

Accepted types of POI

- National ID card
- Passport
- Residence permit card
- Driver’s license
- Citizenship card
- Certified ID
- Birth certificate along with a picture of the user holding the Birth Certificate (If none of the above can be provided this can be used as a last resort)

Proof of Address

- It must be an official (e.g. issued by a government entity or bank) document, containing customer’s full name and full address.
- We residential addresses on the accounts as per regulatory requirements are accepted.
- Must have been issued within the last 3 months.

Accepted types of POA

- Bank statement
- Utility bill
- Property tax receipt
- Local tax bill

- Any ID having the address
- Electoral register
- Back or front of the ID, Driving License (which shows address)

Bank Card (BC)

The type of documents required in this category depends on the method.

- For Credit / Debit / Virtual cards (Visa, MasterCard) a copy of both sides is required showing the BIN (bank identification number) digits, i.e the first 6 digits and the last 4 digits of the PAN (primary account number). The middle digits of the card must be covered for security reasons. Customer must not blank out any details other than the digits not needed. If the customer's name is not printed on the card, then we need a statement that shows the card's digits and the customer's name on the same page. Alternatively, a bank letter stating the card is issued under customer's name, as long as its dated, stamped or signed and its provided-on issuing bank's letterhead.
- For Prepaid cards, the same principles will apply for the player to provide a copy of the card.

Types of Documents for CC (Accepted)

- Visa/MasterCard/Maestro debit or credit card
- Showing first 6 and last 4 digits (PCI)
- Showing full name on card
- Clear copy
- Signature at the back

Ewallet Proof of Ownership (EW SS)

For e-wallets (e.g. Neteller, Skrill) a statement with the full name, account number and email (where applicable) showing to prove ownership of the account.

Types of Documents for EW (Accepted)

- Statement including email/account number and full name

5.2 Appendix B - Source of Funds Verification

The following information is accepted from Customers as Source of Fund/Wealth:

Description of Source by Customer	**Information Required**
Savings from Salary (basic and/or bonus):	Monthly Salary Employer Details Relevant Bank Statements
Insurance Payout/Cashing of Savings Bond:	Amount Received Date received Relevant Bank Statements
Sale of Investments / Liquidation of Portfolio:	Description of Shares / Units / Deposits Relevant Documents Total Amount Received Relevant Bank Statements
Sale of Property:	Sale Documents Total Sale Amount Relevant Bank Statements
Loan	Name of Lender Total Amount Received Loan Agreement Relevant Bank Statements
Inheritance:	Relevant Documents Total Amount Received Relevant Bank Statements
Company Profits:	Name and Address of Company Nature of Business Relevant Bank Statements Net company profits for the last financial year Percentage of ownership

Gift:	Date Received Total Amount Relevant Bank Statements Reason for Gift Relationship to Sender
Other	Specify

5.3 Appendix C - Indicators of Suspicious Activity

Listed below are a number of anti-money laundering risk indicators or "red flags" that might be grounds for suspicion. The list is not exhaustive and not conclusive and can be used as a guide for inquiry and follow-up alongside other material.

A single indicator does not necessarily indicate reasonable grounds to suspect money laundering or terrorist financing activity. However, if several indicators are present during one or a series of transactions, the AML/RFP team will conduct further scrutiny before deciding on whether the transaction must be reported.

Becoming aware of certain indicators could trigger reasonable grounds to suspect that one or more transactions from the past (that had not previously seemed suspicious) were related to money laundering or terrorist financing.

Criteria of Suspicious Transactions

Unusual transactions are identified and reported in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT).

The Company recognises the objective reporting threshold of XCG 5,000 which is identified through transaction monitoring. Transaction monitoring is conducted on an ongoing, risk-based basis. Objective thresholds (including the applicable regulatory indicators XCG 5000) form part of this monitoring framework and serve as triggers for escalation and reporting consideration. In parallel, subjective indicators are applied, where transactions or behaviour give rise to suspicion of money laundering or terrorist financing, regardless of any monetary threshold. All indicators are assessed within the broader context of the customer's risk profile, transactional behaviour, and any additional risk factors, to ensure correct classification and meaningful reporting, including the appropriate sub-indicator and supporting narrative where applicable. Any transaction, including attempted or incomplete transactions, that gives rise to suspicion of money laundering, terrorist financing or other criminal activity shall be reported to the Financial Intelligence Unit Curaçao (FIU Curaçao) without undue delay, regardless of the amount involved.

The Company strictly prohibits tipping-off. Customers are not informed of any internal or external reporting to the FIU Curaçao.The criteria for recognizing money laundering and suspicious operations or transactions related to the behaviour of the Customer includes as follows:

(a) at the time of entering into a business relationship, the Customer is reluctant to provide information necessary to identify the Customer, avoids providing the required personal information, and provides documents which raise doubts as to their genuineness, authenticity etc.

(b) it is difficult to obtain information or documents necessary for the monitoring of the relationship from the Customer: it is difficult to contact the Customer, their place of residence as well as other contact details often change; the phone number provided by the Customer does not answer or it is disconnected; the Customer fails to respond when contacted via email;

(c) the Customer is unable to answer questions regarding their ongoing/planned financial activity and the nature thereof; is excessively nervous;

(d) the Customer expresses a wish to end the business relationship when asked to provide additional information, e.g. source of funds;

(e) at the request of Vanir, the Customer refuses to provide information on the origin of the funds deposited (or an attempted deposit) to their account and/or to support it by relevant documents.

The criteria for recognizing money laundering and suspicious monetary operations are as follows:

(a) the nature of the monetary operations or transactions conducted by the Customer raise a suspicion of efforts to avoid various identification or verification steps set forth by Vanir;

(b) the Customer's account with Vanir appears to be a pass-through account: having deposited the funds to the account, the customer withdraws them shortly afterwards, while other operations barely take place on the account;

(c) during the enhanced review of the Customer's source of funds - the flow of funds and settlements made for them do not match the explanation provided by the Customer;

(d) the Customer makes deposits which are beyond the Customer's possibilities known to Vanir;

(e) the Customer requests that funds belonging to them are paid to persons who are clearly unrelated to the Customer's normal activity;

(f) deposits appear to be made by a Customer using funds from an unrelated third party;

(g) the Customer is subject to financial sanctions in the framework of the Law on the Implementation of Economic Sanctions and other International Sanctions;

(h) the number of deposits from different accounts to the Customer's Vanir account increases without a clear basis;

(i) Customer attempts to register more than one account with the same licensee;

(j) Customer deposits considerable amounts during a single session by means of multiple prepaid cards.

(k) Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.

(l) Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.

(m) Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.

(n) Customer displays suspicious behaviour in playing games that are considered as high risk.

Seeking to recognize the likely features of terrorist financing, the following criteria shall be taken into consideration:

(a) there is information leading to assumption that a Customer does not act for his own benefit and/or may represent a person associated with a risk country or target area, or a person is reluctant to reveal the source of funds;

(b) during a review of a Customer's source of funds, it is identified that the Customer receives or makes or receives remittances to/from the account of a person who is associated with a risk country;

5.4 Appendix D - Jurisdictions

The below list reflects jurisdictions restricted due to licensing, regulatory, or commercial considerations, and is separate from the AML/CFT geographical risk classification outlined above.

Country	**Risk Rating**
Norway	Low
Svalbard and Mayen	Low
Sweden	Low
Åland Islands	Low
Finland	Low
New Zealand	Low

Tokelau	Low
Denmark	Low
Faroe islands	Low
Greenland	Low
Estonia	Low
Slovenia	Low
Lithuania	Low
Malta	Low
Andorra	Low
Saint Pierre and Miquelon	Low
San Marino	Low
Croatia	Medium-High
Austria	Low - Medium
North Mariana Islands	Low - Medium
Bhutan	Low - Medium
Burkina Faso	High
Germany	Low - Medium
France	Low - Medium
French Guiana	Low - Medium
French Polynesia	Low - Medium
Guadeloupe	Low - Medium
Martinique	Low - Medium
Mayotte	Low - Medium
New Caledonia	Low - Medium
Réunion	Low - Medium
Saint Berthélemy	Low - Medium
Saint Martin (French part)	Low - Medium
Wallis and Futuna	Low - Medium
Zambia	Low - Medium
Bermuda	Low - Medium
Montserrat	Low - Medium
Namibia	Medium - High
Mauritius	Low - Medium
Macedonia	Low - Medium
Anguilla	Medium - High
Rwanda	Low - Medium
Solomon Islands	Low - Medium
Brunei Darussalam	Low - Medium
Australia	Low - Medium
Christmas Island	Low - Medium
Cocos (Keeling) Islands	Low - Medium
Norfolk Island	Low - Medium
Czech Republic	Low - Medium
Vatican City State (Holy See)	Low - Medium
Malawi	Low - Medium
Guernsey	Low - Medium

Tonga	Low - Medium
Ireland	Low - Medium
Chile	Low - Medium
Belgium	Low - Medium
Oman	Low - Medium
Singapore	Low - Medium
Fiji	Medium - High
South Korea	Low - Medium
Liechtenstein	Low - Medium
Canada	Low - Medium
Latvia	Low - Medium
Jersey	Low - Medium
Greece	Low - Medium
Poland	Low - Medium
Spain	Low - Medium
Luxembourg	Low - Medium
Lesotho	Low - Medium
Isle Of Man	Low - Medium
British Indian Ocean Territory	Low - Medium
Falkland Islands (Malvinas)	Low - Medium
Pitcairn	Low - Medium
Saint Helena, Ascension and Trista	Low - Medium
United Kingdom	Low - Medium
Taiwan	Low - Medium
Qatar	Low - Medium
Uganda	High
Hungary	Low - Medium
Bulgaria	Medium - High
Micronesia	Low - Medium
Niger	Low - Medium
Slovakia	Low - Medium
Madagascar	Low - Medium
Togo	Low - Medium
American Samoa	Low - Medium
Niue	Low - Medium
Nepal	Low - Medium
Italy	Low - Medium
Romania	Low - Medium
Kuwait	Low - Medium
Switzerland	Low - Medium
Cameroon	High
Gabon	Low - Medium
Bonaire, Sint Eustatius and Saba	Low - Medium
Georgia	Low - Medium
Mauritania	Low - Medium
Papua New Guinea	Low - Medium

Gibraltar	High
Monaco	Medium –High
Sri Lanka	Low - Medium
Ethiopia	Low - Medium
United States Virgin Islands	Medium - High
Chad	Low - Medium
Swaziland (Eswatini)	Low - Medium
Jordan	Low - Medium
Marshall Islands	Low - Medium
Hong Kong	Low - Medium
Portugal	Low - Medium
Congo (Brazzaville)	Low - Medium
Grenada	Low - Medium
Bahrain	Medium
Macau	Medium
Iceland	Medium
Cook Islands	Medium
Bangladesh	Medium
Costa Rica	Medium
Equatorial Guinea	Medium
Aruba	Medium
Nauru	Medium
Puerto Rico	Medium
Timor-Leste	Medium
Argentina	Medium
Indonesia	Medium
Israel	Medium
Gambia	Medium
Maldives	Medium
Cyprus	Medium
Palau	Medium - High
Tuvalu	Medium
Uruguay	Medium
South Africa	High
Suriname	Medium
Guyana	Medium
Turks & Caicos	Medium
Saudi Arabia	Medium
Albania	Medium
Kiribati	Medium
Guam	Medium - High
United Arab Emirates	High
Cote D'Ivoire	Medium
Djibouti	Medium
Seychelles	Medium
Japan	Medium

Peru	Medium
Senegal	High
Malaysia	Medium
Sao Tome & Prin.	Medium
India	Medium
Sierra Leone	Medium
Jamaica	High
Turkey	Medium
Algeria	Medium
Kazakhstan	Medium
Dominican Republic	Medium
Cayman Islands	Medium
Angola	Medium
Vanuatu	High
St Vincent & Gren	Medium
El Salvador	Medium
Thailand	Medium
Honduras	Medium
Tajikistan	Medium
Eritrea	Medium
St Maarten	Medium
British Virgin Islands	Medium
Kyrgyzstan	Medium
St Kitts & Nevis	Medium
Barbados	Medium - High
Uzbekistan	Medium
Benin	Medium
St Lucia	Medium
Moldova	Medium
Antigua and Barbuda	Medium - High
Mexico	Medium
Botswana	Medium
Dominica	Medium
Cape Verde	Medium
Colombia	Medium
Tanzania	High
Kosovo	Medium
Turkmenistan	Medium
Paraguay	Medium
Guinea	Medium
Curacao	Medium
Mongolia	Medium
Samoa	Medium - High
Montenegro	Medium
Belize	Medium
Serbia	Medium

Mozambique	High
Kenya	Medium - High
Guatemala	Medium
Comoros	Medium
Vietnam	High
Philippines	High
Morocco	Medium - High
Western Sahara	Medium - High
Bolivia	Medium - High
Cuba	Medium - High
Belarus	Medium - High
Lao People's Democratic Republic	Medium - High
Tunisia	Medium - High
China	Medium - High
Armenia	Medium - High
Ecuador	Medium - High
West Bank (Palestinian Territory)	Medium - High
Mali	High
Liberia	Medium - High
Ukraine	Medium - High
Gaza Strip	Medium - High
Azerbaijan	Medium - High
Central African Rep	Medium - High
Nigeria	High
Brazil	Medium - High
Russian Federation	High
Burundi	Medium - High
Sudan	Medium - High
Egypt	Medium - High
Bosnia-Herzegovina	Medium - High
Nicaragua	Medium - High
Ghana	Medium - High
Myanmar	High
Trinidad & Tobago	High
Bahamas	High
Congo, the Democratic Republic	High
Cambodia	High
Panama	High
Haiti	High
Venezuela	High
Zimbabwe	High
Libya	High
South Sudan	High
Guinea Bissau	High
Pakistan	High
Iraq	High

Lebanon	High
Somalia	High
Syria	High
Yemen	High
Afghanistan	High
North Korea	High
Iran, Islamic Republic of	High

5.5 Appendix E - Banned Countries

The following is a list of banned jurisdictions from which we neither accept nor permit any real money wagering or play on our site:

Afghanistan, Albania, Algeria, American Samoa, Angola, Anguilla, Antigua & Barbuda, Argentina, Armenia, Aruba, Australia, Azerbaijan, Bahamas, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin, Bermuda, Bhutan, Bonaire (Sint Eustatius and Saba), Bosnia And Herzegovina, Botswana, Bouvet Island, British Indian Ocean Territory, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Cape Verde, Cayman Islands, Central African Republic, Chad, Christmas Island, Cocos (Keeling) Islands, Colombia, Comoros, Congo (Democratic Republic of), Cook Islands, Costa Rica, Cote d'Ivoire, Croatia, Cuba, Curacao, Cyprus, Czech Republic, Djibouti, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Ethiopia, Falkland Islands (malvinas), Faroe Islands, Fiji, France, French Guiana, French Polynesia, French Southern Territories, Gabon, Gambia, Ghana, Gibraltar, Greece, Greenland, Grenada, Guadeloupe, Guam, Guatemala, Guinea, Guinea-Bissau, Guyana, Haiti, Heard Island, Holy See (Vatican City State), Honduras, Hong Kong, Iran (Islamic Republic of), Iraq, Israel, Italy, Jamaica, Jordan, Kazakhstan, Kosovo, Kyrgyzstan, Lao People's Democratic Republic, Latvia, Lesotho, Liberia, Libya, Lithuania, Madagascar, Malawi, Malaysia, Maldives, Mali, Marshall Islands, Martinique, Mauritania, Mauritius, Mayotte, Mexico, Micronesia, Montenegro, Montserrat, Mozambique, Myanmar, Namibia, Nauru, Nepal, Netherlands, Netherlands Antilles, New Caledonia, Nicaragua, Niger, Nigeria, Niue, Norfolk Island, North Korea, Northern Mariana Islands, Oman, Pakistan, Puerto Rico, Réunion, Romania, Rwanda, Saint Barthélemy, Saint Helena, Saint Helena, Saint Kitts & Nevis, Saint Lucia, Saint Martin, Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Samoa, San Marino, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Singapore. Saint Maarten, Slovakia, Slovenia, Solomon Islands, Somalia, South Georgia and the South Sandwich Islands, South Sudan, Spain, Sri Lanka, State of Palestine, Sudan, Suriname, Svalbard and Jan Mayen, Swaziland, Switzerland, Syria, Taiwan, Tajikistan, Tanzania, Timor-Leste, Togo, Tokelau, Tonga, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan Turks and Caicos, Tuvalu, U.S. Virgin Islands, Uganda, United Kingdom, United States Minor Outlying Islands, United States of America (and its dependencies), Uzbekistan, Vanuatu, Venezuela, Virgin Islands, Wallis And Futuna, Western Sahara, Yemen, Antarctica, Macedonia, Moldova, Mongolia, Kenya, Kiribati and Lebanon

5.6 Appendix F - Transaction monitoring rules

Vanir Ventures B.V has the below rules available through its player account management system (PAM). In combination with the “indicators of suspicious activity” in appendix 4.3, they are used to monitor transactions and prevent ML & TF.

Rule	**Description**
ALREADY_REGISTERED_CARD	If the card was previously registered on a different account, then it cannot be added on another account
BIN_COUNTRY_MISMATCH	If the card is issue by a bank from a different country than the one registered as address
BIN_IP_MISMATCH	If the IP is from a different country than the one registered as address
BLACKLISTED_CC_RULE	If the card that is being registered was already flagged as fraudulent by the system/agent in the past
BLACKLISTED_IP_RULE	If the IP from where the customer is registering was already flagged as fraudulent by the system/agent in the past
CC_COUNTS	If the customer uses XX or more different cards to deposit in X time

CC_NAME_MISMATCH	If the name registered on the account does not match with the name registered with the card
DEPOSIT_AMOUNT	If the total amount deposited is XX or more in a timeframe of XX
DEPOSIT_AMOUNT_CHECK_ BEFORE_KYC	If a player tries to deposit more than the set limit within the defined period before KYC approval then this risk rule will be violated.
DEPOSIT_CHECK_AFTER_KYC	If a player tries to deposit more than the set limit within the defined period after KYC approval then this risk rule will be violated.
DEPOSIT_COUNT_CHECK_ BEFORE_KYC	This risk rule will be violated if the Count of Deposits (per transaction Status) say X made by the Player in specific period say Y exceeds the Count Value defined before KYC
DEPOSIT_COUNT_STATUS_WISE	The risk will trigger upon reaching certain count in a specific time frame with a specific transaction status
EMAIL_LINKED_RULE	This risk rule will be violated if the count of unique email addresses registered by all the linked accounts of player exceeds "X" within "Y" time.
IOVATION_RULE	Iovation is a 3rd party tools that offers information if the customer is flagged there. Yes/No
IP_CHANGE	This risk rule will be violated if the player has changed his login IP at least once in the specified period in the Rule
LOGIN_IP_COUNTRY_USER_ COUNTRY_ MISMATCH	The current log in IP country does not match with the user country

LOGIN_IP_MISMATCH_WITH_ LAST_LOGIN_ RULE	The current log in IP country does not match with the previous login IP
PAYMENT_IP_COUNTRY_ MISMATCH	The Payment method is registered in a different country than the user country
SIMILAR_PLAYER	If the player is having any existing linked account related to: · FNAME_LNAME_PASSWD_RULE · ADDRESS_RULE · FNAME_LNAME_DOB_RULE more than X amount of times
USED_IP	This risk rule will be violated if the player has logged in with an IP that is already used by some other Player in XX minutes
WHITE_LIST_CARD	These white listed cards will be exempted from the configured risk rules
WHITE_LIST_EMAIL	These white listed emails will be exempted from the configured risk rules

6. Abbreviations

AML – Anti-Money Laundering

CFT – Combating the Financing of Terrorism

AML/CFT – Anti-Money Laundering and Combating the Financing of Terrorism

KYC – Know Your Customer

CDD – Customer Due Diligence

EDD – Enhanced Due Diligence

ML – Money Laundering

TF – Terrorist Financing

PF – Proliferation Financing

UTR – Unusual Transaction Report

FIU Curaçao – Financial Intelligence Unit Curaçao

goAML – United Nations Office on Drugs and Crime reporting system used by FIU Curaçao

MLRO – Money Laundering Reporting Officer

Deputy MLRO – Deputy Money Laundering Reporting Officer

RFP – Risk, Fraud and Payments Department

CAP – Client Acceptance Policy

PEP – Politically Exposed Person

POI – Proof of Identity

POA – Proof of Address

IBAN – International Bank Account Number

BIN – Bank Identification Number

PAN – Primary Account Number

CVV – Card Verification Value

PAM – Player Account Management System

FATF – Financial Action Task Force

CGA – Curaçao Gaming Authority

NORUT – National Ordinance on the Reporting of Unusual Transactions

LOK – National Ordinance on Games of Chance

All employees are required to acknowledge that they have read, understood and will comply with this Policy.

For any questions regarding this Policy, employees may contact:

Christos Pitsoulis

GROUP MLRO

Email: christos@vanirventures.com

Signed by:
8737E2B30CF043F...
Analissa Heiland

Signed by:
E9C1A4A3F74E4ED...
Lorenza Godett

Directors on behalf of Xecutive Corporate Management B.V.