

AML/CFT & KYC Policy

Issuer: VANIR VENTURES B.V.

Version: 1.0

Date: 02/07/2024

Table of Contents

1. Introduction	4
1.1 Purpose	4
1.2 Scope	5
1.2.1 Employee's mission	5
1.2.2 Vanir's Mission:	5
1.3 Annual Review & Records Retention	6
1.4 Money Laundering and Terrorist Financing	6
1.4.1 What is Money Laundering?	6
1.4.2 Stages of the ML process:	6
2. AML/CFT & KYC Policy	7
2.1 Initial Customer Registration	7
2.1.1 Preventing Underage Gaming	7
2.2 Customer Risk Assessment	7
2.3 KYC Thresholds	7
2.3.1 Verification	7
2.3.2 Customer Due Diligence ("CDD")	8
2.3.2.1 Verifying Identity	8
2.3.2.2 Acceptable documents for Identity	8
2.3.2.3 Acceptable documents for Address Verification	8
2.3.2.4 Verification of Customer's Payment Method	8
2.3.3 Enhanced Due Diligence ("EDD")	9
2.3.3.1 Verifying the Source of Funds	9
2.3.3.2 Acceptable documents for Source of Funds Verification	9
2.3.3.3 Further EDD Reviews	10
2.3.4 Risk Based Approach	10
2.3.4.1 Ongoing Monitoring	10
2.4. Client Acceptance Policy:	11
3. Document Checking Procedure	11
3.1 Suspicious Activity Reporting	13
4. Appendix	14
4.1 Appendix A - Acceptable Documents for Identity Verification	14
4.2 Appendix B - Source of Funds Verification	15

4.3 Appendix C - Indicators of Suspicious Activity	17
4.4 Appendix D - Jurisdictions	19
4.5 Appendix E - Banned Countries	24
4.5 Appendix F - Transaction monitoring rules	25

DS DS



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 5th AML Directive as well as further guidance supplied by the Curacao Gaming Authority are the primary pieces of legislation that drive the Vanir KYC framework.

DS DS



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;

1.2 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:

1.2.1 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.

1.2.2 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 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.

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:

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.

DS DS



2. AML/CFT & KYC Policy

2.1 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.

2.1.1 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.

2.2 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 criteria used for risk assessment may be found in the Customer Risk Assessment Policy.

2.3 KYC Thresholds

2.3.1 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.

Upon reaching the €2K threshold, the Customer is put through the Customer due diligence (“CDD”) process.

DS DS



2.3.2 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 (i.e. the customer, his/her geographic location, transaction volumes, frequency of play and behaviour) as well as (b) Transaction Risk – which focuses on the complexity and size of transactions being made. On the basis of these categories, rating of low, medium or high risk allocation is made about a customer. At Vanir, standard CDD is applied to customers who carry a low or medium risk. Customers are asked to provide documentation confirming their identity, address and ownership of payment methods (where applicable). Vanir can also request the customer to hold the ID card next to their face, and other measures, if deemed necessary.

The events that trigger the CDD procedure are as follows:

- 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)

2.3.2.1 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.

2.3.2.2 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.

2.3.2.3 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.

2.3.2.4 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.

2.3.3 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

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 or lawful purposes.

2.3.3.1 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.

2.3.3.2 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.

2.3.3.3 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;

2.3.4 Risk Based Approach

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.

2.3.4.1 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.

2.4. 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.

3. 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.

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

DS DS



information collected to that point is forwarded to the MLRO for further review and a potential filing of a Suspicious Transaction Report.

i. The Customer is not informed of these suspicions and subsequent actions.

3.1 Suspicious Activity Reporting

The value of SARs is wide-reaching. Some SARs provide immediate opportunities to stop crime and arrest offenders, others help uncover potential criminality that needs to be investigated, while others provide intelligence useful in the future. All contribute to strategic threat assessment.

Information provided through SARs such as contact details, alias identities, investment activity, bank accounts, and other assets can lead to the instigation of new investigations or enhance on-going operations.

Persons working in the regulated sector are required under the Proceeds of Crime Act and the Terrorism Act to submit a SAR in respect of the information that comes to them in the course of their business if they know, or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing.

You may commit an offense if you have ‘knowledge’ or ‘suspicion’ of a money laundering activity or criminal property, and doing something to assist another in dealing with it and failing to make a SAR.

We analyze the SARs to extract strategic and tactical intelligence, to identify the most sensitive SARs, and send them to the relevant authorities for investigation.

Reporters of SARs would not routinely be provided with updates on their SARs.

Kindly include as many details as you can as it could become a valuable piece of Information. Poor quality reporting can lead to unnecessary delays.

You can ask the MLRO for the SAR template. Please send all SARs to christos@vanirventures.com

DS DS



4. Appendix

4.1 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

4.2 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

4.3 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

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;

DS DS



4.4 Appendix D - Jurisdictions

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

DS DS



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

DS DS



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

DS DS



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

4.5 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,

DS DS



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

4.5 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

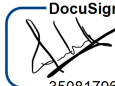
PAYMENT_IP_COUNTRY_MISMATCH	The Payment method is registered in a different country than the user country
SIMILAR_PLAYER	If the player is having any existing linked account related to: · FNAME_LNAME_PASSWD_RULE · ADDRESS_RULE · FNAME_LNAME_DOB_RULE more than X amount of times
USED_IP	This risk rule will 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

DocuSigned by:



E9C1A4A3F74E4ED...

DocuSigned by:



3508179679034CB...

Lorenza Godett and Christopher Van Rosberg
Directors obo Xecutive Corporate Management B.V.

AML/CFT & KYC Policy

Issuer: Project Vanir Ltd

Version: 1.0

Date: 03/07/2024

Table of Contents

AML/CFT & KYC Policy 1

1. Policy Statement 3

1.1 General clauses 3

2. Our Mission 4

3. Definition of Money Laundering 5

4. What is Terrorist financing? 5

5. Key element of our KYC process includes the following non-exhaustive list of objectives: 5

6. Cases where the Company may cease the provision of services to Customers: 6

7. Training and Awareness Program 6

7.1 Aims of training program 6

7.2 Training Components: 7

8. Recruitment 7

9. Risk Assessments 7

9.1 Risk Factors Considered: 7

9.2 Client Risk: 7

10. Customer Due Diligence 8

11. Enhanced Customer Due Diligence 8

12. Politically Exposed Personal (PEP's) 8

13. Sanctions Compliance 9

14. Behavioural Triggers 10

15. Investigation Process 10

16. Standard Precautions 11

17. Record Keeping 12

18. Official Reporting Lines 12

18.1 Suspicious Activity Reporting 12

18.2 Whistleblower Policy 13

19. Revisions and Review 13

Project Vanir Ltd

Voukourestiou, 25 Neptune House, 1st floor, Flat/Office 11 Zakaki

3045, Limassol, Cyprus

Registration No. HE 454098

Company: Project Vanir Ltd (hereinafter "Project Vanir" and/or the "Company")

Registry code: HE 454098

Members of the management board: XCM Services Ltd

1. Policy Statement

Project Vanir has chosen to instigate best practice policies, procedures and structures to improve its handling of Money Laundering Issues and Know Your Customer (hereinafter this policy and procedure referred to as "KYC") Practices.

These have been drawn-up to work within the best practice principles and guidelines supplied from several international standards, directives and acts. These include but are not limited to:

- FATF Recommendations (Financial Action Task Force, European Inter-governmental body)
- Estonian Money Laundering and Terrorist Financing Prevention Act
- Guidelines regulating money laundering issues issued by the Estonian Financial Intelligence Unit.

The aforementioned policies and reporting procedures, along with the implied quality standards, apply internationally across Project Vanir and its associated companies.

The Prevention of Money Laundering and Terrorist Financing Manual (hereby referred to as the "Manual") is issued by Project Vanir in accordance with "The Prevention and Suppression of Money Laundering Activities Law of 2007 (L.188(I)/2007), as amended and the Estonian Money Laundering and Terrorist Financing Prevention Act as entry into force on 27.11.2017 (collectively, the "Applicable Laws").

The commitment and compliance with this Manual is the responsibility of all the Company's employees. The program of the Manual includes amongst other things, Politically Exposed Persons ("PEPs") and sanctions screening of customers, on-going monitoring of customers and transactions, policies and procedures of the Know Your Customer principle ("KYC") and Customer Due Diligence ("CDD"), record keeping, reporting suspicious activities and training employees on ML/TF issues.

Furthermore, the Company has processes in place to ensure:

- (1) its AML program and guidance remains up to date with regulatory changes,
- (2) there is a continuity program notwithstanding any changes to its management or employee composition, and
- (3) there is proper reporting to its senior management/Board of Directors.

1.1 General clauses

DS


All employees of the Company are required to familiarise themselves with the Estonian Money Laundering and Terrorist Financing Prevention Act, the guidelines issued by the Estonian Financial Intelligence Unit in respect of money laundering issues and this KYC Policy.

All relevant employees should regularly follow information and notifications published on the website of

Estonian Financial Intelligence Unit:

<https://www2.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/>

All relevant employees to whom the Manual applies, shall be personally responsible for the due fulfilment of the requirements prescribed in the Estonian Money Laundering and Terrorist Financing Prevention Act.

This Manual should be always available to all the employees of the Company.

This Manual is developed and periodically updated by the Anti-Money Laundering Compliance Officer based on the general principles set up by the Company's Board of Directors in relation to the prevention of Money Laundering and Terrorist Financing. This Manual aims to outline the obligations of the senior management and staff of the Company under the provisions of the Law.

The Manual shall be communicated by the MLRO to all the employees of the Company that manage, monitor or control in any way its customers' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined.

The purpose of the Manual is to lay down the Company's internal practice, measures, procedures and controls relevant to the prevention of Money Laundering (ML) and Terrorist Financing (TF) and further assist the Company's employees to achieve the following objectives:

- a. Implement and comply with all the legal and regulatory requirements that govern the operations of the Company.
- b. Maintain the integrity, credibility and reputation of the Company.
- c. Enable the tracking and identification of suspicious transactions/activities and protect the company from possible fraud and risks involved in its financial strength and reputation.
- d. Report any suspicious transactions/ activities of ML, TF or PF internally and externally to the appropriate authorities.
- e. Be able to contribute to the investigation, if a customer of the Company is investigated for ML or TF and submit data on the specific incident.
- f. Enable the development of the professional relationship with its customers.

The Company has appointed Christos Pitsoulis to undertake the duties of the Compliance Manager and Money Laundering Reporting Officer (MLRO). The MLRO will report all suspicious transactions to the relevant authorities (e.g. Estonian Financial Intelligence Service). All suspicious transactions on player accounts should be reported internally to the MLRO.

Player accounts showing such suspicious activity will be reviewed and escalated where required to the Financial Intelligence Service (FIS).

Access to emails that report or flag suspicious activities, should be restricted to the Money Laundering Reporting Officer and such other employees or officers of the Company that strictly require or need to be notified of such matters. . All transactions in relation to any suspicious activity will be kept for a minimum period of 5 years as from when the transaction was performed and will be made available to the relevant authorities on request.

2. Our Mission

Employees' Mission:

- Strict adherence to the provisions of this Manual

DS


- Identification and examination of unusual transactions
- Identify, assess and manage risks
- Proper record keeping
- Rigorous application of the principles of KYC

Company's mission:

- To have mechanisms in place to report suspicious transactions.
- To establish criteria and develop clear acceptance policies and procedures for new and existing customers of the business.
- To have mechanisms in place to be able to prevent and identify suspicious transactions when they take place.; and
- To identify the Company's risk areas and ensure that adequate controls are in place to mitigate those risks.

3. Definition of Money Laundering

- Money Laundering is a term given to the various methods by which individuals attempt to make illegally earned money appear legitimate and to facilitate the evasion of a variety of taxes. The definition of money laundering has expanded to include the movement of funds for the purpose of supporting terrorist activities.
- Pursuant to Estonian Money Laundering and Terrorist Financing Prevention Act "Money laundering" means:
 - a. Concealment or maintenance of the confidentiality of the true nature, origin, location, manner of disposal, relocation or right of ownership or other property-related acquired as a result of a criminal activity or property acquired instead of such property;
 - b. conversion, transfer, acquisition, possession or use of property acquired as a result of a criminal activity or property acquired instead of such property with the purpose of concealing the illicit origin of the property or assisting a person who participated in the criminal activity so that the person could escape the legal consequences of his or her actions.

Money laundering also means a situation whereby a criminal activity, as a result of which the property used in money laundering was acquired, occurred in the territory of another state.

Money Laundering is no longer simply the act of 'cleaning' or making respectable the proceeds of crime. It is now widely understood that the generic term is now used to additionally cover any proceeds from criminal activities. Therefore the goal of anti-money laundering activities is to eradicate profit from criminal activity including, narcotics trafficking, fraud, embezzlement, corruption and trafficking in human beings and 'cyber crime'.

4. What is Terrorist financing?

"Terrorist financing" means financing acts of terrorism as defined in § 237.3 of the Penal Code. 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.

5. Key element of our KYC process includes the following non-exhaustive list of objectives:

- a. Customer Identification: Provision of valid and up-to-date identification documents or information to establish their identity. This may include government-issued IDs, passports, or other legally recognized forms of identification.
- b. Address Verification: Provision of utility bills, bank statements, or similar documents.

DS 

- c. Source of Funds: Information/documentation in regards to the Source of funds used for gambling activities to ensure that they are legitimate and not derived from illicit activities.
- d. Enhanced Due Diligence: In cases where customers exhibit higher-risk characteristics, such as large transactions or PEP status or high risk country, we will conduct enhanced due diligence to gain a deeper understanding of their background and financial activities.
- e. Ongoing Monitoring: KYC is not a one-time process. We continuously monitor customer transactions and behaviours to detect and report any suspicious or unusual activities.

6. Cases where the Company may cease the provision of services to Customers:

- a. In the event that the customer has breached any of the Company's terms and conditions governing the use of its services.
- b. If the customer is involved in criminal or suspicious activities, due to a criminal conviction or any other cause that may cause a brand or reputation damage to the Company.
- c. In the event of the customer's death
- d. Customers who fail and/or refuse to submit, upon the review of the customer's file, the requisite data and/or information for the purpose of completing the CDD and KYC measures and procedures and there is no other third party source to obtain or request information.
- e. The Company decides to discontinue the provision of services for whatever reason it thinks appropriate.
- f. If, during the review/customer update process, the customer fails and/or refuses to provide vital information requested by the Company.
- g. If a client has attempted to deceive the Company in any way by reason of information submitted or answers to given.

7. Training and Awareness Program

The Company seeks to ensure that all efforts are made to identify customers who:

- a. Reach substantial transaction levels — deposit and withdrawal.
- b. Behave in a fashion that deviates from the 'norm' and therefore arouses suspicion.

Therefore, all staff who have involvement with customers and customer accounts and transactions are required to undergo a training program to ensure that they are fully aware of issues and the reporting structure available to them. The training program involves providing a complete understanding of the 'normal' patterns and what constitutes suspicious activity or questionable activity deviating from the 'norm'.

Customer Service Representatives will not be required, nor trained to deal with investigative procedures. Their job specifications require them to place the customer first. Requesting them to question customers or investigate them would create a conflict.

The dedicated Fraud Investigations Team work with the Customer Service Representatives. They are trained to understand and deal with the types of investigation required to further identify suspicious behaviours and what steps to take to clarify issues before further reporting.

In most cases simple investigations will clarify issues and either offer a simple explanation or provide the basis for further investigation and reporting within the structure provided by the Company.

Yearly updates and refresher courses are made available to existing staff. This enables staff to be made aware of any issues that have arisen and how they were dealt with.

7.1 Aims of training program

Our training program is designed to ensure that our employees have sufficient knowledge of:

- 1. Risk Recognition: education of employees on how to recognize red flags and indicators of potential money laundering, fraud, or other illicit activities.

DS


2. Legal and Regulatory Compliance: Emphasis on the importance of adhering to applicable laws and regulations, and provide guidance on how to stay current with regulatory updates.
3. Reporting Procedures: training on the correct procedures for reporting suspicious activities and transactions through the designated reporting channels (MLRO).
4. Comprehensive Understanding: All employees, from entry-level to management, will receive training to develop a comprehensive understanding of AML/KYC regulations.

7.2 Training Components:

1. New employees will undergo mandatory AML/KYC training as part of their onboarding process.
2. Depending on their roles within the Company, some employees will receive specialized training tailored to their responsibilities.
3. Regular refresher courses and updates will be provided to ensure that employees stay up to date about changes in regulations and emerging risks.

The MLRO also receives frequent training on the latest methods used by criminals for money laundering, continuous update of applicable Law and Directives, Sanction Screening and other compliance Matters for detecting and Preventive Money laundering.

8. Recruitment

All new employees are recruited from reputable and known agencies, via local contacts or promoted from within the Company. The agencies require all employees to have suitable references and the Company further requires that all new employees who are offered a permanent or temporary contract are asked to provide two sources of independent referees.

These independent referees are then sent a letter (and/or telephoned) to ensure that the prospective employee's details are correct.

All new employees within the above teams are provided with a comprehensive course to suit their job role and will all undergo induction training which includes Anti Money Laundering.

9. Risk Assessments

The company has assessed the risk of money laundering and terrorist financing taking into account the policies and controls that are currently in place. The highest staking (and therefore highest depositing customers) (so-called VIP's) will be analysed separately*. /This system will be developed in due course./ These customers have a 'one to one' relationship with territory managers and gives added assurance that risk of money laundering and terrorist financing is low. The company will continue to monitor the exposure of the business to money laundering as to keep it up to date with the changing environment and technologies.

9.1 Risk Factors Considered:

Product and Service Risk: The types of casino products and services and their susceptibility to money laundering or fraudulent activities

Customer Risk: The client and the geographic location, transaction volumes, and behaviour.

Transaction Risk: The complexity and size of transactions.

9.2 Client Risk:

Finally, depending on the above risk factors of a customer, the customer will be allocated with one of the following Risk Ratings:

1. Low Risk
2. Normal Risk
3. High Risk

10. Customer Due Diligence

All Customers should undergo KYC procedures if they meet one of the following criteria:

1. Single deposit exceeding €2,000 (or equivalent)
2. A series of deposits, in excess of €2,000 (or equivalent)
3. Single withdrawal in excess of €2,000 (or equivalent)
4. A series of withdrawals, in excess of €2,000 (or equivalent)

Customers who already have documentation on file may be requested for updated documentation if details change on their account. For identity and address verification purposes, the following documents should be obtained from the Company's customers:

❖ Identity verification:

Passport and/or national identity card and/or valid driving license which must clearly indicate:

- a. Photograph of the individual
- b. Document number and type
- c. Date of issue
- d. Expiry date
- e. Country of issue
- f. Date of birth

❖ Address Verification:

Either of the following documents:

- a. Utility bill, up to 6 months dated
- b. Bank statement up to 6 months dated
- c. Tax Assessment
- d. Residence permit

NB: Clients that use Bank ID as authentication are automatically Identified and verified using that deposit method.

11. Enhanced Customer Due Diligence

The Company shall apply the following EDD measures:

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 where there are high volumes as well as amounts of transactions
4. In other cases of higher risk that are identified by the Company

The company shall apply EDD measures in the above situations in order to manage and mitigate those risks appropriately. The Company shall 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 or lawful purpose.

12. Politically Exposed Personal (PEP's)

A "politically exposed person" is a natural person who performs or has performed prominent public functions, their family members and close associates. A person who, by the date of entry into a

DS


transaction, has not performed any prominent public functions for at least a year, and the family members or close associates of such person are not considered politically exposed persons.

A "person performing prominent public functions" is:

- a. a head of state, head of government, minister, deputy minister or assistant minister;
- b. a member of parliament;
- c. a justice of a supreme court, constitutional court or another court the judgments of which can be appealed against only in exceptional circumstances;
- d. a member of the supervisory board of a state audit institution or central bank;
- e. an ambassador, charge d'affaires and senior officer of the Defence Forces;
- f. a member of a directing, supervisory or administrative body of a state-owned company.

The definition includes positions in the European Union and in other international organisations. A family member of a person performing prominent public functions is:

- a. his or her spouse;
- b. a partner equal to a spouse under the law of the person's country of residence or a person who as of the date of entry into the transaction had shared the household with the person for no less than a year;
- c. his or her children and their spouses or partners within the meaning of clause 2);
- d. his or her parent.

A "close associate of a person performing prominent public function" is:

- a. a natural person who has a close business relationship with a person performing prominent public functions or with whom a person performing prominent public functions is the joint beneficial owner of a legal person or contractual legal arrangement;
- b. a person who as a beneficial owner has full ownership of a legal person or contractual legal arrangement, which is known to have been founded for the benefit of the person performing prominent public functions.

The company has enlisted a third party provider that supplies an online tool to trace and identify PEPs. Where a PEP has been identified, senior management approval will be obtained to for that customer to continue to be registered.

Enhanced customer due diligence will be the requirement to obtain additional identification data to verify the identity of the customer and/or the source of their funds (see documentation requests below).

13. Sanctions Compliance

Vanir is committed to complying with all applicable economic and trade sanctions laws and regulations, including those imposed by the United Nations, European Union, United States, and other relevant jurisdictions. This Sanctions Policy outlines the procedures and responsibilities for ensuring compliance with these regulations.

Vanir prohibits any activities that would violate sanctions laws, including transactions with individuals, entities, or countries subject to sanctions. All employees must be vigilant in identifying and reporting potential sanctions violations.

Vanir will screen all clients, counterparties, and transactions against applicable sanctions lists to ensure compliance. Regular updates of sanctions lists will be maintained, and screening processes will be adjusted accordingly. Enhanced due diligence will be conducted for clients and transactions involving high-risk countries or entities, and due diligence records will be maintained for at least five years.

Any potential sanctions violations must be reported immediately to the Money Laundering Reporting Officer (MLRO) via email at christos@vanirventures.com. The MLRO will assess the reported issue and determine if a full investigation is necessary. Confirmed violations will be reported to relevant regulatory authorities as required.

Regular training will be provided to all employees on sanctions compliance, including how to identify and report potential violations. Training records will be maintained for audit purposes. All records related to sanctions screening, due diligence, and reporting will be kept for a minimum of five years and will be accessible for audits and regulatory inspections.

The MLRO is responsible for overseeing the implementation of the sanctions policy, conducting or coordinating investigations into potential violations, ensuring protection and confidentiality for individuals reporting potential violations, and maintaining records of all sanctions-related activities and training. All employees are required to adhere to this policy, report suspected violations, and cooperate with the MLRO during investigations.

14. Behavioural Triggers

It should be noted that suspicious behaviour triggers further investigation. At all times the customer should be treated with courtesy and where possible, the customer should be kept unaware of any investigations.

In cases of financial risk or suspected fraud, the Fraud Department will take appropriate steps to protect funds.

This list below provides examples of suspicious behavioural patterns that trigger further investigation. There is a constant review of behavioural patterns.

1. Large amounts of money deposited within 48 hours of account opening;
2. Large deposits, little activity, withdrawal requested to a different method than deposit;
3. Deposit amounts are out of the 'Norm' when compared to the demographic profile;
4. Focus purely on multiplayer games, or dual player games and only with the same people within a 24 hour period;
5. Withdrawal Bank Account used by other Accounts;
6. Claimed address country differs from IP trace.
7. Withdrawal requested to name / address / personal details which differ from registration details.
8. The customer has deposited and played during relatively short period of time considerable amounts (more than 20 000 euros per month).
9. The person requests that written confirmation will be issued to third party for the prizes won.
10. The person pays deposit with the credit card issued to the governmental authority or other similar authority or with the card, which is not linked to any natural person.
11. The person requests, after short period of playing for the remaining deposit (more than 2000 euros), to be paid out and requests also confirmation letter for the pay-out.

15. Investigation Process

During the establishment of customer relationship, the following data in respect of Estonian residents will be gathered:

- a. First name and surname;
- b. Personal identification code;
- c. Personal identification document no, issuer, place and date of issuance (digital ID certificate details);
- d. Place of residence, address;
- e. Place of work (professional field of activity);
- f. Phone number

In respect of Estonian residents, compulsory online identity verification system is established with cooperation with AS Sertifitseerimiskeskus or similar service.

In case behavioural triggers occur, Project Vanir may ask from customer presentation of additional documents.

Required proof of identity — must include copies of the following:

1. Passport or Driving License or National Identity Card
2. Proof of Address — Utility Bill / Official or Bank Correspondence
3. Proof of ownership of account — Bank Statement or Card Statement (figures may be blocked out).

These documents will be preferably sent in digital format signed with person own digital signature. The company may ask these documents also in notarized format (whereby the validity (originality) of the document is confirmed by the notary public). Documents will be stored on a secure drive, which only members of the fraud department can access. Any hard copy documentation is filed and stored in a locked filing cabinet of which only senior members of the fraud department have access.

The information should be checked against all available databases.

Relevant documentation is kept for minimum 5 years as of last transaction with the customer and for a maximum of 7 years in line with current data protection act.

In certain situations, it may be necessary to establish the source of funds and the wealth of the customer, or ask other information in respect of nature of the transaction, aim of transaction etc.

The company will use all reasonable efforts to obtain this information.

Customers IP address information will be stored in respect of every transaction.

During the establishment of client relationship following data in respect of FOREIGN RESIDENTS will be gathered:

- First name and surname;
- Personal identification code, date of birth, place of birth;
- Travel document details, issuer, date of issuance, place of issuance;
- Place of residence, address;
- Place of residence in the moment of establishing contact with Project Vanir
- Area of professional activity (place of work);
- Information whether person can be considered as PEP;
- Phone number.

The customer will be requested to present documents confirming the identity.

Required proof of identity — must include copies of the following:

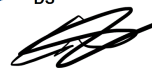
1. Passport or Driving License or National Identity Card
2. Proof of Address — Utility Bill / Official or Bank Correspondence
3. Proof of ownership of account — Bank Statement or Card Statement (figures may be blocked

The company may ask presentation of these copies in notarized format (whereby the validity (originality) of the document is confirmed by the notary public). Documents will be stored on a secure drive, which only members of the fraud department can access. Any hard copy documentation is filed and stored in a locked filing cabinet of which only senior members of the fraud department have access.

The information should be checked against all available databases. Customers IP address information will be stored in respect of every transaction.

16. Standard Precautions

There are standard rules governing Deposits and Withdrawals that act as an immediate 'common sense' barrier to Money Laundering.

DS


First withdrawals should be sent to the source of deposits wherever possible, regardless of the amount. Secondly, where possible, ensure there is a level of personal contact, albeit by phone.

17. Record Keeping

A database of all accounts closed or with action taken by the fraud team is kept on our internal systems with access only available to the fraud team. All supporting hard copy documentation is stored in a secure filing cabinet in the main fraud team office. All data is kept for a minimum of 5 years and for maximum of 7 years.

18. Official Reporting Lines

Where investigations leave further suspicions, all available information will be gathered and taken to the Financial Institution involved in the transactions.

All suspicious transactions will be reported to MLRO, who will then review and analyse them, and forward if deemed necessary to the appropriate Financial Intelligence Service, no later than 2 (two) working days after the activity or circumstances have been identified or suspicion has arisen.

18.1 Suspicious Activity Reporting

The value of SARs is wide-reaching. Some SARs provide immediate opportunities to stop crime and arrest offenders, others help uncover potential criminality that needs to be investigated, while others provide intelligence useful in the future. All contribute to strategic threat assessment.

Information provided through SARs such as contact details, alias identities, investment activity, bank accounts, and other assets can lead to the instigation of new investigations or enhance on-going operations.

Persons working in the regulated sector are required under the Proceeds of Crime Act and the Terrorism Act to submit a SAR in respect of the information that comes to them in the course of their business if they know, or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing.

You may commit an offense if you have 'knowledge' or 'suspicion' of a money laundering activity or criminal property, and doing something to assist another in dealing with it and failing to make a SAR.

We analyse the SARs to extract strategic and tactical intelligence, to identify the most sensitive SARs, and send them to the relevant authorities for investigation.

Reporters of SARs would not routinely be provided with updates on their SARs.

Kindly include as many details as you can as it could become a valuable piece of information. Poor quality reporting can lead to unnecessary delays.

You can ask the MLRO for the SAR template. Please send all SARs to christos@vanirventures.com

Contact details – online reports:

<https://www.politsei.ee/et/saada-teade>

MLRO will be reporting in accordance to the rules established with the Estonian Money Laundering and Terrorist Financing Prevention Act and guidelines published by the Estonian Financial Intelligence

Unit available: <https://www.riigitataja.ee/akt/101122017020>

Where money has been received from a bank account, we will approach them with our concerns, or if it is a request for withdrawal we will approach the bank that holds the account that would receive the funds. This enables us to ensure that we adhere to local Financial Regulations and that the correct Authorities are informed.

DS


MLRO is aware that he may publish information relating with the suspicious transactions/data only to:

1. The management board of Project Vanir and employee appointed by the management board;
2. Estonian Financial Intelligence Unit;
3. Investigation authorities during the criminal procedure;
4. Court on the basis of the judgement or regulation.

The Person suspected may not be informed.

18.2 Whistleblower Policy

This Whistleblower Policy encourages and protects individuals reporting suspected unethical, illegal, or improper conduct related to anti-money laundering (AML) compliance.

Reports can be made through email to christos@vanirventures.com (MLRO email). All reports will be treated confidentially, and the whistleblower's identity will be protected by the MLRO.

Retaliation against whistleblowers is strictly prohibited. Any form of retaliation will result in disciplinary action. The MLRO will conduct an initial assessment to determine if a full investigation is needed. Investigations will be conducted impartially, and the MLRO will report findings and recommended actions. The whistleblower will be informed of the outcome, if possible.

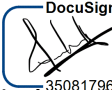
All Vanir employees are encouraged to report suspected unethical conduct to the MLRO and cooperate with investigations conducted by the MLRO. Vanir's management is responsible for promoting transparency and accountability and protecting whistleblowers from retaliation.

The MLRO's responsibility is to oversee the whistleblower program, conduct or coordinate investigations, and ensure protection and confidentiality for whistleblowers.

19. Revisions and Review

This Policy will be reviewed on a regular basis to ensure that all of the latest amendments to the money laundering regulation are kept up to date.

The Policy will be reviewed and approved by the management board of Project Vanir Limited.

DocuSigned by:

3508179679034CB...
Christopher Van Rosberg
Director obo XCM Services Ltd