Versus Odds B.V.

Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) Policy

CONFIDENTIALITY STATEMENT

This is a confidential document for Versus Odds B.V. It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the organization without written approval of Versus Odds B.V.

Disclaimer

Contact

Versus Odds B.V.
Mark Cauchi
+356 2166 0939
compliance@kmlpartners.com

Document Version Control

Versus Odds B.V. – AML/CTF Policy	
VERSION CONTROL	
Current version	2.2
Effective Date	2025-04-25
Sign Off Date	2025-04-25
Document Owner	Senior Compliance Officer / MLRO
Next Review Date	2026-04-24
Comments	The policy will be reviewed on the following basis: No less than once annually, with such review to be initiated by the Policy owner approximately one month prior to the date following 12 months from which the procedure was last approved. • In response to any changes in relevant regulation and/ or legislation. • In response to general guidance notes or best practice guidance issued by any relevant regulator. • In response to any regulatory action taken • In response to findings of a relevant internal or external audit; or • Upon request of management.
Purpose	Amendments to reflect regulatory requirements according to the AML Policy template guidelines

Version history

Version	Date	Author	Purpose
1.0	2024-05-23	Versus Odds B.V.	Creation of the firs AML/CTF Policy
2.0	2024-08-01	Versus Odds B.V.	Creation of a new up to date AML/CTF Policy
2.1	2024-10-17	Versus Odds B.V.	Update of the AML/CTF Policy
2.2	2025-04-25	Versus Odds B.V.	Amendments to reflect regulatory requirements according to the AML Policy template guidelines published by the CGA

Table of Contents

1. Introduction & Background

1.1 Scope & Purpose

The provisions in this Anti-Money Laundering Policy (this "Policy") aim to reduce the possibility for the business of providing services by Versus Odds B.V. to be used for criminal purposes or in violation of regulations.

Versus Odds B.V. is a Curaçao licensed online gaming entity.

Being a remote gaming entity authorized under Curaçao jurisdiction, Versus Odds B.V. is deemed to be carrying out "relevant financial business" in terms of the CGA's AML/CFT/CFP Regulations and thus Versus Odds B.V. is a subject-person in terms of said Regulations. As such, it is required to abide by the applicable legislation and guidance relating to the prevention of money laundering and funding of terrorism.

This Policy provides guidance detailing responsibility regarding the prevention of money laundering and funding of terrorism from the perspective of the legal framework of Curaçao and internationally accepted regulations in this area. This information includes due diligence, monitoring, training and record-keeping policies and procedures, as well as a description of the role and responsibilities of the Compliance Officer.

1.2 Definitions

1.2.1 Money Laundering

"Money laundering" means:
All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement;
- Layering; and
- Integration.

1.2.2 Terrorist financing

"Terrorist financing" or "Financing of Terrorism" means:
Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

1.2.3 Financing of Proliferation of weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

1.2.4 Targeted Financial Sanctions

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

1.3 Definition of "Client" and "Applicant for Business"

The direct client of Versus Odds B.V. and applicant for business shall be the player who enters into an agreement with the Company - or with a group company which who a service agreement is in place - by virtue of registration, agreeing to the Terms & Conditions, and funding the player account in order to utilize the Versus Odds B.V. platform to play games remotely.

For the avoidance of doubt, a player who has registered and agreed to the Terms & Conditions but has not yet funded his player account is not considered to be an applicant for business.

In this scenario, an intermediary of Versus Odds B.V., who shall enter into a business relationship with Versus Odds B.V. for the purpose of attracting players to Versus Odds B.V., shall also satisfy the definition of applicant for business.

1.4 Audience

This AML Policy applies to all employees, officers, directors, contractors, consultants, and any other individuals or entities acting on behalf of the Company, regardless of location or job function.

It is particularly relevant for individuals engaged in the following activities:

- Customer onboarding and due diligence
- Financial transactions and payment processing
- Compliance and risk management
- Legal and regulatory affairs Internal audit and controls
- Sales and account management

All personnel must understand their responsibilities under this policy and complete any required AML training provided by the Company. Failure to comply with the obligations outlined in this policy may result in disciplinary action, up to and including termination of employment or contract.

Third-party partners, agents, and service providers who represent or act on behalf of Versus Odds B.V. may also be required to comply with this policy, as determined by the nature of their relationship with the company.

1.5 Law, Regulations and Rules

The Code of Criminal Law (Penal Code) of Curaçao lays down the procedures for the prosecution of a money laundering offence, as well as the measures for the confiscation of property upon a conviction of money laundering, measures for the freezing of assets when a person is charged with an offence of money laundering and measures for the issuance of an investigation and/or attachment order when a person is suspected of having committed an offence of money laundering.

The policies and procedures in this Policy aim to comply with both the rules and guidance contained in the NOPML, the NORUT and the NOIS which regulations themselves are referring to the Penal Code. In addition to these regulations the Curaçao Gaming Board has introduced a comprehensive framework with provisions and guidelines to prevent and combat money laundering and terrorist financing. Curaçao - as a member of the FATF - has based these guidelines on, among others, the FATF recommendations.

1.6 Document Structure

Each section below is divided into the following parts:

a) The applicable provisions in the NOPML, the NORUT and the NOIS or and CGA regulations;
b) Guidance on the implementation (where applicable);
c) Versus Odds B.V.'s policy in relation to the provisions; and
d) Procedures and Documentation – the processes by which the policy referred to will be implemented, including reference to other documents as appropriate.

1.7 Consequences of non-compliance

Violations of this AML Policy can expose the Company, its employees, and its partners to significant legal, regulatory, and reputational risks. Understanding and complying with this policy is essential to protect the integrity of our operations and to fulfill our legal and ethical obligations.

Disciplinary Actions

Any employee who fails to comply with this policy may be subject to disciplinary action, which may include:

- Formal warnings;
- Suspension;
- Termination of employment or contract;
- Loss of professional licenses or certifications.

Contractors or third parties found in violation may face termination of agreements and disqualification from future business with Versus Odds B.V.

Legal Implications

Non-compliance with AML regulations can result in severe legal consequences, including:

- Civil or criminal prosecution;
- Substantial fines and financial penalties;
- Imprisonment of individuals involved;
- Asset seizures or freezing of funds;
- Disqualification from serving as a company officer or director.

Business and Reputational Risks

Violations can also damage the company's reputation, investor confidence, and customer trust. Potential consequences include:

- Regulatory investigations or sanctions;
- Loss of partner relationships;

- Increased scrutiny from financial authorities;
- Negative media exposure and reputational harm;
- Financial loss due to operational disruptions or terminated business relationships.

2. AML Systems and Controls – General

2.1 Provisions from the Nois and the Norut

Due Diligence should be applied:

i) When establishing business relations;
ii) Where there is a suspicion of ML or TF;
iii) Where there is doubt about the veracity or adequacy of previously obtained identification data.

The Company is obliged to apply the above measures and procedures including the cases when entering into or undertaking non-face-to-face relationships or transactions directly or indirectly.

The Company is also obliged to establish policies and procedures on risk management practices, internal controls, record keeping, and the monitoring and management of compliance with the aforesaid policies, controls and procedures to adequately and appropriately mitigate risk and prevent the carrying out of operations that may be related to money laundering or the funding of terrorism.

The Company must ensure that employees are made aware of applicable AML/CFT legislation as well as the Company's policies and measures in this regard. Employees of the Company must undergo appropriate due diligence procedures prior to their engagement, when transferred or when promoted. Employes are also expected to be provided with training regarding the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

2.2 Policy

Responsibility

The ultimate responsibility for the AML policy of Versus Odds B.V. lies with the Director(s). Day-to-day responsibility for the development and implementation of policies and procedures contained within this Policy is delegated to the Key Compliance Officer/MLRO.

AML policies and procedures

The policies and procedures operated by Versus Odds B.V. in order to meet applicable AML and CFT regulatory requirements are documented in this Policy. Policies and procedures will be regularly reviewed to ensure that they continue to meet regulatory requirements and the changing risk environment as per Versus Odds B.V. as far as applicable.

AML Risk

The Compliance Officer/MLRO will undertake regular assessments of the money laundering risks and Versus Odds B.V.'s strategy and success in mitigating those risks.

Versus Odds B.V. will document its risk management policies and risk profile in relation to money laundering, and its application of those polices in this Policy and in subsidiary documentation referenced herein.

Versus Odds B.V. uses the following guidance as a base for its AML risk model:

i. a clear statement of the culture and values adopted towards the prevention of financial crime;
ii. a commitment to ensuring that identity will be satisfactorily verified in all cases and in a risk based manner, before applicants for business are accepted as clients;
iii. a commitment to ongoing customer due diligence throughout the business relationship;
iv. a commitment to ensuring that staff are trained and aware of the law, their legal obligations, and how to meet those obligations
v. a clear allocation of roles, responsibilities and organizational structure, and recognition of the importance of staff promptly reporting their suspicions internally.

2.3 Procedures and documentation

Responsibility

The delegated day-to-day responsibility for the AML policy and operation of effective procedures of the Company is documented in the Compliance Officer / MLRO's Job Description in Annex I below.

Responsibility for the review and update of the AML Policy, and applicable sections, rests with the Compliance Officer/MLRO and can be delegated to local MLRO if any. Each version of the AML Policy will be reviewed and approved by the Board of Directors prior to being issued and will carry a review and approval date.

AML policies and procedures

The AML Policy is subject to Versus Odds B.V.'s local and group policies and procedures regarding compliance monitoring, record keeping and reporting.

The AML Policy is reviewed as necessary (but at least annually), updated in order to reflect changes in legislation, national and international findings, the structure of Versus Odds B.V.'s customers, and the services offered.

The procedures contained in this Policy reflect the Versus Odds B.V. AML Policy in general and are more specific with respect to the jurisdiction Curaçao and must be adhered to by all staff of the companies belonging to Versus Odds B.V.

AML risk factors

An AML business risk assessment overview will be maintained in order to allocate and track the components of the separate risk classifications. Versus Odds B.V. categorizes overall AML risk into:

- Customer risk;
- Geographical risk;
- Product, service and transaction risk; and
- Distribution channels risk

As part of the periodic review of this AML Policy, the Compliance Officer / MLRO will periodically assess the AML risk for each category in order to develop appropriate mitigating controls. See Annex II – Risk Assessment below:

Document	Title	Frequency	Audience	Resp.
AML Policy, Annex I	MLRO Job Description	Periodic	MLRO, Directors	MLRO
AML Policy, Annex II	Risk Mitigation Matrix and Risk Factors	Periodic	MLRO, Directors	MLRO

3 Risk Assessment, Management and Risk-Based Approach

3.1 Provisions of the NOIS

The Company is required to have policies and procedures in place to mitigate specific risks involved with business transactions or non-face-to-face transactions.

Based on the FATF recommendations and CGA guidelines service providers are allowed to apply a Risk-based Approach (“RBA”). By adopting an RBA, it is possible for service providers to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risk identified. This entails that although all clients should be subject to minimum due diligence standards clients identified by the service provider as high risk must be subject to enhanced customer due diligence while low risk clients may be subject to the simplified minimum prescribed customer due diligence.

3.2 Guidance on Implementation

Risk Assessment

For the implementation of risk-assessment procedures, the AML Regulations recognizes the FATF Standards and that the Company should prepare a risk-assessment, as well as policies, controls, and procedures curated to manage and mitigate ML/FT risks.

The purpose of the risk-assessment procedures is to enable the Company to be in a position to identify and assess the ML/TF risks that the Company is or may become exposed to and thereby determine:

a) Whether the application of enhanced due diligence is necessary;
b) The point in time when the application of customer due diligence in accordance with the NOIS to existing customers is to be carried out; and
c) Whether a customer presents a low risk of ML/FT for the purposes of delaying the performance of verification proceedings to after the commencement of a business relationship, as has been discussed above.

Monitoring Controls

It is essential that the controls to manage and mitigate the identified risks are constantly monitored. This should be done so that in the event of a change in circumstances, which might mitigate or exacerbate a particular risk, the respective control is modified accordingly.

For instance, it is important that the Company has a system in place to identify changes in customer characteristics, as this would obviously have a bearing on the risk profile of the customer. Similarly, the threat posed by a particular product or service may cease to exist, which would lead to a re- consideration of the risk scoring of the business relationship. In view of this, the Company must be in a position to identify such changes.
The Company should also carry out periodic internal audits or assessments to review the adequacy of the risk assessment, the internal controls and the compliance arrangements. Such audits or assessments should also review the effectiveness of liaison between the different departments of the organization, and the effectiveness of the balance between technology-based and people-based systems.

3.3 Policy

Risk-based approach

Versus Odds B.V. operates a risk-based approach to developing and operating its systems and controls designed to prevent financial crime.

AML risk is analyzed, as applicable, into the following risk categories:

- Customer risk;
- Geographical risk;
- Product, service and transaction risk; and
- Distribution channels risk.

The Risk Assessment and Mitigation Matrix in Annex II to this Policy identifies and explains the risks inherent to the particular services provided by Versus Odds B.V., as well as the actions taken by the Company to mitigate these risks.

The Risk Factor table also in Annex II to this Policy identifies risk factors relevant to Versus Odds B.V.'s business that indicate a risk of money laundering or terrorist financing.

Risk assessment for the customers is initiated upon reaching the sum of Naf 4,000 (Eur 2,000) with accumulative withdrawal threshold and continuously monitored and re-assessed within the high-risk category. The procedure for arriving at a risk category is set out in Annex II below.

AML risk assessment

The Compliance Officer/MLRO will perform regular assessments of the AML risks and Versus Odds B.V.'s local strategy and success in mitigating those risks.

Where a new service, customer group or new geography is addressed by Versus Odds B.V., the financial crime risk assessment will be updated during development/launch (to ensure that AML processes can support the new activities). In line with article 5h of the NOIS the company will assure that affiliated entities will meet the Curaçao Anti Money Laundering and Terrorist Financing regulations. Such as far as these affiliated entities are affecting the business of the Company in Curaçao. The results of the AML risk assessment will be used to support the development of appropriate systems and controls (policies and procedures) designed to minimize the risk of Versus Odds B.V., being used for the purposes of financial crime. All developments will be reported to the Board of Directors.

Risk mitigation

In order to mitigate the risk of money laundering, Versus Odds B.V. will ensure that appropriate risk-based systems and controls are in place and operated for, amongst others, the Company as prescribed in Annex II below. Existing systems and controls will be reviewed and where necessary amended to reflect changes in assessed risk and identified vulnerabilities. Additional systems and controls will be implemented by the MLRO where required.

Monitoring controls

The AML Policy is subject to Versus Odds B.V. policies and procedures regarding compliance monitoring. The MLRO will ensure that the internal controls operated by Versus Odds B.V. are reviewed when there are changes to regulations or Versus Odds B.V.'s arrangements / products / markets.

When there is a change in the Versus Odds B.V. AML policies or AML rules in the CGA's AML Regulations this Policy, and associated materials, will be updated and details of the changes included in the MLRO's Annual Report.

3.4 Procedures & Documentation

Risk-based approach

The application of the RBA in the prevention of money laundering is reflected in the Versus Odds B.V.'s approach to the operation and development of the systems and controls designed to minimize the risk of the Versus Odds B.V. being used for the purposes of financial crime. Risk is central to the development of the business, new products, development of product functionality or the operation in new markets. The risk-based approach is referenced in all Versus Odds B.V.'s AML documentation.

AML risk assessment

AML risk assessments are undertaken on an ongoing basis, and in particular, applied when the business environment changes through, for example:

- Entry into new markets; and
- Development of new products or product features / functionality.

Risk mitigation activities, i.e. the development of appropriate internal controls, flow from the findings of the risk assessments.

Risk assessments and the development of mitigating actions are documented in Annex II below and are accordingly reported to the Board of Directors.

Risk mitigation

Versus Odds B.V. seeks to minimize the opportunities for carrying out financial crime, i.e. money laundering or funding of terrorism, and to then address and mitigate any risks that remain as further set out in Annexes II and III below.

Internal controls focus on:

- Due diligence of clients, including levels of enhanced due diligence based on risk assessments of each customer;
- Assessing risks and setting out measures to mitigate the said risks;
- Monitoring key risk factors for reassessing a specific customer's risk;
- Financial crime systems and controls will continue to be developed over time in order to adequately address the changing risk environment.

Monitoring controls

This Policy is reviewed and, if necessary, updated continuously in order to reflect changes in the AML policies and procedures which affect the operations of Versus Odds B.V. Consequently, the MLRO's regularly reviews the following areas.

a) Developments in legislation, including the NOIS; and the NORUT.
b) Financial crime risk assessments – whose performed as part of the development

of new products, services, functionality or addressing new customers / markets.

c) The operation of periodic internal controls, including monitoring, investigation and reporting of unusual activity.
d) New typologies for fraud or financial crime, including feedback from regulators or law enforcement.
e) Feedback received following the provision of training or Compliance reports to the Board by the MLRO.

Document	Title	Frequency	Audience	Responsibility
Report	MLRO Internal Audit Report	Annual	Board	MLRO

4. Customer Due Diligence

4.1 Guidance from CGA Regulations

Casinos have the obligation to undertake Customer Due Diligence measures when:

a) When players engage in financial transactions equal to or above Naf. 4,000;
b) carrying out occasional transactions above the monetary equivalent of NAf. 4,000;
c) there is a suspicion of money laundering or terrorist financing; or
d) the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

4.2 Guidance on implementation

The CDD measures to be taken are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds.

Notwithstanding this, the NOIS allows subject persons to delay the verification of the identity of the applicant for business and, where applicable, the identity of the beneficial owner until after the establishment of a business relationship where this is necessary for the continued normal conduct of business provided that the risk of money laundering or the funding of terrorism is low and, provided further, that the verification procedures be completed as soon as is reasonably practicable after the initial contact. Regulations add that in the event that customer due diligence measures are applied after the establishment of a business relationship, subject persons should record the reasons for deferring the application of customer due diligence measures. A determination on whether the risk of money laundering or funding of terrorism is low should be based on mandatory risk procedures.

4.3 Policy

Customers of the Company are subject to risk-based initial and ongoing due diligence procedures according to the risk categories outlined in Annex II below and the Customer due diligence procedures set out in Annex III below.

Initial due diligence seeks to obtain the identity of the customer and verify the identity prior to the establishment of the business relationship. Information on the purpose and intended nature of the business relationship, is also obtained, such that the Company is able to establish the business and risk profile of the customer and to accept or reject a client based on the Client Acceptance Policy set out in Annex IV below. Ongoing procedures ensure that the initial due diligence information remains up to date.

4.4 Procedures and Documentation

The detailed procedures for the performance of risk-based customer due diligence are detailed in Annex III below relating to Customer Due Diligence.

Document	Title	Frequency	Audience	Responsibility
AML Policy, Annex II	Risk Mitigation Matrix and Risk Factors	As required	Relevant staff	MLRO
AML Policy, Annex III	Customer Due Diligence	As required	Relevant staff	MLRO
AML Policy, Annex IV	Client Acceptance Policy	As required	Relevant staff	MLRO
Terms and Conditions	Services Agreement	As required	Relevant staff	MLRO

5. Ongoing monitoring

5.1 Provisions from the Regulations

The casino must conduct ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the casino's knowledge of the customer, the customer's business and risk profile.

5.1.1 Ongoing monitoring of identity

"In conducting ongoing due diligence on the business relationship the casino should hold accurate and up to date identification data of its customers. Since identity may change due to circumstances, the casino should be able to demonstrate that if identification information changes, it will be detected and re-evidenced."

5.1.2 Ongoing monitoring of transactions

"Transaction monitoring is executed to prevent involvement of the casino with ML/TF and to safeguard the reputation of the casino. While performing ongoing scrutiny of transactions a casino notices that a customer's transactions are not consistent with what it knows or expects from the customer, the casino has to question this unusual activity and, where necessary, establish the source of the funds used for these transactions."

5.2 Guidance on Implementation

The NOIS states that once the business profile of a customer has been established, ongoing monitoring enables subject persons to identify any unusual transactions which may involve ML/FT. This gives greater assurance that the activities of the subject person are not being misused for the purposes of ML/FT. The regulations provide further that ongoing monitoring of a business relationship includes:

a) the scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds; and
b) ensuring that the documents, data or information held by the subject person are kept up to date.

Paragraph (a) above requires subject persons to collect the necessary information to ensure that the customer's business corresponds to the information disclosed by the customer at the beginning of the business relationship and that the business patterns of the customer are consistent with the risk profile established by the subject person. Where it is revealed that the customer's business and risk profiles have significantly diverged from the established patterns or for no apparent economic or lawful purpose, action should be taken in accordance with the internal procedures of the subject person. This should be conducive to reviewing the risk profile of the customer and considering whether reporting is necessary.

Thus, as a result of the introduction of systems and procedures to ensure ongoing monitoring, activities which do not conform to the established business and risk profiles of the customer are immediately brought to the attention of the MLRO. The MLRO would then be in a position to assess whether there is a suspicion of ML/FT and whether that suspicion warrants a report to the FIU in terms of article 2d of the NOIS and article 11 paragraph 1 of the NORUT.

In order to fulfil the obligation, set out in paragraph (b) above, subject persons are required to have a system in place to keep up-to-date documents, data or information held in the fulfilment of their CDD obligations, including information and documents obtained by the subject person. in order to fulfil the obligation set out under article 6 of the NOIS. This should include the updating of expired documentation. This ensures that in the event of an analysis or investigation of ML/FT the subject person is in a position to provide accurate and updated information to the FIU or the Police.

5.3 Policy

Ongoing monitoring processes will focus on ensuring that due diligence information provided is up to date and that no documentation is expired. On-going monitoring will also ensure that there have been no material changes to the Client that affects the risk profile of the Client.

On-Going Monitoring Measures
On-Going Monitoring will be conducted on a continual basis for all Customers. On-Going Monitoring will include:

- Ongoing Screening: Daily/Weekly screening against all relevant sanctions, PEPs, and adverse media lists.
- Periodic Review: Periodic Reviews will be commensurate to the ML/TF risk associated with the Customer.
- Event Driven Reviews ("EDR"): An EDR will be initiated on the identification of a high-risk factor or red flag during the ongoing monitoring process (including Transaction Monitoring).

<u>Due Diligence information</u>

Due diligence information will be reviewed as follows to ensure that it remains up to date.

Low Risk Customers: Once every 2 years
Medium Risk Customers: Annually
High Risk Customers: Quarterly

5.4 Procedures and Documentation

The Company notes that it offers a single service to its customers whereby the applicant for business is affecting payments for remote gambling services. Therefore, in all cases, the Company understands the nature of the relationship with the customer and all payments received are sourced from this business.

Training will be provided to relevant staff to ensure that they are aware of the requirement to stay alert to the possibility of unusual activity and what unusual activity might comprise. Training is addressed in Section 9 below.

Customer initial due diligence information set out in Annex III will be periodically reviewed to ensure that it remains up to date as per the above. This review is recorded by way of assessing whether any due diligence information has expired.

The review will also assess whether any changes have been made to the company structure and/or the people involved. In such an instance, due diligence will be updated accordingly.

6 Reporting

6.1 Provisions from the CGA's AML regulation

Casinos are not only required to adhere to the stipulations of the National Ordinance for Identification of Services, but are also required to detect and report either intended or completed unusual transactions. It is important that every casino has adequate procedures in place that cover the following:

- The recognition of unusual transactions;
- The documentation of unusual transactions; and
- The reporting of unusual transactions.

As regards external reporting, the NORUT provides:

Where a subject person knows, suspects or has reasonable grounds to suspect that a transaction may be related to money laundering or the funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism, or that money laundering or the funding of terrorism has been, is being or may be committed or attempted, that subject person shall, as soon as possible, disclose that information, supported by the relevant identification and other documentation, to the Financial Intelligence Analysis Unit.

6.2 Guidance on Implementation

Internal Reporting
If the MLRO concludes, for justifiable reasons, that an internal report does not give rise to a suspicion, the MLRO need not to inform the FIU. In this case, the MLRO shall keep a written record of the internal reports received, the assessment carried out, the outcome and the reasons why the report was not submitted to the FIU. Upon request by the FIU or the relevant supervisory authority acting on behalf of the FIU, or in completing the Annual Compliance Report, the MLRO will make such information available.

Offences Committed Outside Curaçao

According to article 5h paragraph 1 of the NOIS the Service Provider should take care and organize that its foreign subsidiaries and branches, if any, are meeting the requirements of the NOIS. In case and as far as the legislation of the involved jurisdiction does not allow the NOIS measures the Service Provider should inform the Regulatory Authority followed by actions of the Service Provider to avoid the risks of ML/TF.

6.3 Policy

Annual Compliance Report and MLRO Report

Each casino has to register with the FIU and to obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore the casino account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

The Compliance Officer / MLRO shall also prepare a report to be presented to the Directors to outline issues pertinent to the management of financial crime, of which the Board should be aware. This MLRO Report is for internal purposes and does not need to be submitted to the FIU.

Internal Reporting

Versus Odds B.V.'s reporting policy applies to the 'relevant staff' of Versus Odds B.V., Providers and Distributors. Relevant staff are those that handle or who are managerially responsible for handling, or are otherwise 'close', to customer transactions or accounts.

Versus Odds B.V. will generate two types of unusual activity reports:

- **Internal UTRs** - Internal unusual activity reports may be generated by all relevant staff. Internal UTRs are used to report unusual activity to the MLRO, and
- **External UTRs** - External unusual activity reports are produced by the MLRO in the event of unusual activity having been identified and confirmed through investigation. External UTRs are submitted to the FIU. *Each casino has to register with the FIU and to get access to the goAML reporting portal after validation by the FIU.*

Records relating to both Internal and External UTRs are kept in accordance with Versus Odds B.V.'s record- keeping policy. External UTRs are kept for a minimum period of 5 years.

All relevant staff will receive both initial and ongoing training on anti-money laundering, detection of unusual activity and the internal reporting process.

Internal Reporting - Versus Odds B.V. Staff

Where a Versus Odds B.V. staff member knows or suspects, or has reasonable grounds for knowing or suspecting, that any customer is engaged in money laundering, they must report these suspicions to the MLRO using the Versus Odds B.V. Unusual Transaction Reporting Form.

Any Versus Odds B.V. staff member that does not adhere to the internal reporting requirements will be subject to disciplinary process.

Internal Reporting – Providers and Distributors

Where any relevant staff member in a Provider or Distributor, knows or suspects, or has reasonable grounds for knowing or suspecting, that any customer is engaged in money laundering, they should report their suspicion directly to the Versus Odds B.V. MLRO.

External Reporting (MLRO)

Where an unusual activity report has been made to the MLRO he will conduct investigations and access information on the customer, or the transaction, as necessary.

Where appropriate, an UTR will be made to the FIU by the MLRO which will include the mandatory information. In the file format and following the instructions available from the FIU. The UTR can be filed through the FIU's goAML portal or by means of a manual report form (http//: www.mot.cw).

6.4 Procedures and Documentation

MLRO Role

The responsibilities associated with the MLRO role are documented in the MLRO Job description.

To ensure that Versus Odds B.V. maintains an AML approach that meets regulatory requirements, the MLRO will regularly review developments in legislation and their impact on the policies and procedures contained in this Policy, including:

1. Curaçao legislation (CGA regulations);
2. National and International Findings; and
3. Local legislation in the countries of relevant Providers and Distributors.

If changes in the Curaçao anti-money laundering legislation are found to contribute to an increased risk of money laundering, through the periodic performance of a financial crime risk assessment, the policies and procedures in this Policy will be updated by the MLRO. The MLRO communicates changes in policies and procedures to all relevant parties.

In order to ensure that Versus Odds B.V. AML approach addresses current AML risk, the MLRO undertakes regular financial crime risk assessments and considers the Versus Odds B.V. strategy and success in mitigating those risks, using the risk categories detailed in Annex II. The performance of risk assessments is detailed in Section 3 above. The results of these periodic assessments will be regularly reported to the Board of the Company.

Internal Reporting

Relevant staff will receive initial and periodic training to ensure that their reporting obligations, and the method of making an Internal UTR, are understood as well as to assist them to recognize unusual activity. Typologies are maintained and will be used as part of the training provided.

Internal UTRs should be sent to the MLRO using the 'Versus Odds B.V. Unusual Transaction Reporting Form'. The MLRO acknowledges the receipt of all Internal UTRs and will provide a reminder regarding tipping off requirements to the person making the report.

The MLRO will investigate all reported unusual transactions in light of all available information and document the findings, regardless of whether or not an external UTR is made. All documented information will be retained with the Versus Odds B.V. Unusual Transaction Reporting Form and retained in order to provide documentary evidence of the investigation process. Any further attempted activity on an account where an internal UTR has been made must be reported to the MLRO to ensure that appropriate action is taken in order to avoid tipping off.

External Reporting

An external UTR is triggered when, after investigation by the MLRO, a transaction, transaction pattern or account activity is deemed unusual and suggests potential criminal activity. External UTRs will be sent to the Curaçao FIU.

7 Record-Keeping Procedures

7.1 Provisions from the NOIS and the NORUT

Regulation of the NOIS provides that the following records are to be kept for a period of at least five years by the subject person:

a) in relation to any business relationship that is formed or an occasional transaction that is carried out, a record indicating the nature of the evidence of the customer due diligence documents required and obtained under procedures maintained in accordance with these regulations, comprising a copy of or the reference to the evidence required for the identity and providing sufficient information to enable the details as to a person's identity contained in the relevant evidence to be re-obtained;
b) a record containing details relating to the business relationship and to all transactions carried out by that person in the course of an established business relationship or occasional transaction which shall include the original documents or other copies which are admissible in court proceedings;

c) a record of the findings of the examination of the background and purpose of the relationships and transactions therein.

7.2 Guidance on Implementation

The regulations provide that generally, records may be kept in any of the following forms:

- in physical files;
- in scanned form;
- in computerized or electronic form.

Subject persons should use a standardized approach to record keeping and must ensure that the approach used enables the quick retrieval of records.

7.3 Policy

The MLRO is responsible for specifying which AML records must be retained and for ensuring that all such records are retained in accordance with Versus Odds B.V.'s record-keeping policy. Records may be held in paper-based and/or electronic form and stored by the Company. The Company will ensure that all AML records are retrievable without undue delay.

Records must be kept for a minimum of **5 years** (may be extended to 10 years if required by the FIU). The table below provides guidance on the types of records that must be retained and their respective retention periods.

7.4 Procedures & Documentation

The below timeframes do not relate to accounting records which, in terms of Book 2 of the civil code of Curaçao are to be retained by the company for a period of 10 years:

Record	Content	Location	Responsibility
Outsourcing	SLAs or contracts, details of contact persons, training records, any relevant information about local anti-money laundering legislation.	Versus Odds B.V.	Key Official
Record of Customer Due Diligence	Identity of clients; Identity of directors, beneficial owners, business proposition, expected transaction levels	Versus Odds B.V.	MLRO

Internal & external unusual transaction reports	All actions, information not acted upon, UTRs made	Versus Odds B.V.	MLRO
AML Training	Dates, nature of training, names of attendees, results. To be stored in the personnel files.	Versus Odds B.V.	MLRO
AML Policy	Previous versions of the AML Policy	Versus Odds B.V.	MLRO

8. Awareness and Training

8.1 Provisions from the NOIS

Casinos must take appropriate measures from time to time for the purpose of making employees aware of said subject person's AML/CFT policies and procedures as well as relevant legislation.

The NOIS also provide that a subject person must provide "...employees from time to time with training in the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism."

8.2 Guidance on Implementation

Regulations state that all employees should be made aware of the subject person's:

- customer due diligence measures;
- record-keeping procedures;
- internal reporting procedures;
- policies and procedures on internal controls;
- policies and procedures on risk assessment and risk management; and
- policies and procedures on compliance management and communication.

Employees should also be made aware of the following:

- CGA regulations (including the provisions of the NORUT and the NOIS);
- the provisions in the Criminal Code on ML & TF;
- the provisions of the P&G;
- the offences and penalties in relation to any breach of the NOIS or the NORUT

All the above-mentioned information should be made readily available to all employees to enable them to refer to such information as and when appropriate throughout the conduct of their duties.

The P&G highlights that training should be tailored in accordance with the specific responsibilities and functions of the respective employees and the business carried out by the subject person. For instance, front-office employees should be provided with a different kind of training to that provided to employees carrying out back-office functions and the training provided by a credit institution would naturally differ from the training provided by a company carrying out the business of insurance or a real-estate agent.

Additionally, training should be of a more practical nature rather than simply theoretical. This means that the training provided should make references to real-life situations such as, for instance, the steps to be followed when accepting customers, the handling of high-risk customers and the behavior to be adopted when faced with a request for a transaction which is suspicious. Typology reports prepared by the FATF or Moneyval play an important role in preparing training material.

Casinos need to determine the method in which training is to be delivered, as the most appropriate method may vary from one organization to the other. The method generally depends on the size of the organization. Online learning systems can often provide an adequate solution for general training to all employees who deal with clients, while focused classroom training for higher- risk areas can be more effective.

It is vital to maintain comprehensive records of training sessions which, should include:

a) the date on which the training was delivered;
b) the nature of the training;
c) the names of employees receiving the training;
d) the results of any assessment undertaken by employees; and
e) a copy of any handouts or slides.

8.3 Policy

The Versus Odds B.V. MLRO is responsible for ensuring that all relevant staff received training that effectively communicates Versus Odds B.V.'s AML and CFT responsibilities and the policies and procedures that are operated to ensure that those responsibilities are met.

Relevant persons

Relevant staff include the staff of the Company who handle or are managerially responsible for the handling of customer on-boarding and service provision.

Training

Training will be designed to ensure that all relevant staff are made aware of the risk of the Company being used for the purposes of financial crime, the consequences for the firm (as well as staff personally), the requirement to operate systems and controls to mitigate such risk and the requirement to report unusual activity to the MLRO.

The frequency of the provision of AML training will be determined using a risk-based approach, with those who may be at greatest risk from handling unusual transactions, or who need to be kept up-to-date with changing vulnerabilities and trends, receiving training at more frequent intervals; relevant staff who are close to transaction processing activity are prioritized for training which may be more detailed in content than the training provided for other staff.

Where applicable, provision for AML training will be made in the contractual arrangements, or Service Level Agreements, between Versus Odds B.V. and its partners.

MLRO training

The MLRO will keep up to date with legislative changes in Curaçao and on international level and industry standards in order to guide and develop appropriate training for relevant staff.

8.4 Procedures & Documentation

Relevant persons

The MLRO will maintain a record of Versus Odds B.V. staff, and their positions within the company, for use when deciding which individuals are 'relevant staff' and, further, which will require more frequent and more detailed training due to the nature of their specific role.

Training

All relevant staff will be provided with an awareness of Versus Odds B.V.'s AML policies and processes through the provision of AML training. Relevant staff will be provided with initial AML training within one month of their taking up relevant activities on behalf of Versus Odds B.V. Priority is given to those staff responsible for handling or managing the handling of transactions or customer accounts.

All relevant staff must acknowledge that they have read and understood the training that is provided, to be recorded in the AML Staff Training Log.

The frequency of training provided to each staff member is determined by the MLRO with reference to the staff member's role. Refresher training is repeated at appropriate intervals. Relevant staff are tested on the AML training received.

Training materials are updated by the MLRO when required to reflect new developments. Training materials and records are retained in accordance with the Company record-keeping policy.

AML training will be delivered to relevant staff and will include the following elements:

1. Legal and regulatory obligations under Curaçao law;
2. Practical means of identifying unusual transactions; and
3. Internal processes and advice on how to act when presented with unusual activity.

MLRO training

The MLRO will receive external training as appropriate and is required to evidence, to the Board, their further professional development (using the MLRO Annual Report).

Document	Title	Frequency	Audience	Responsibility
Presentation	AML Awareness & Training Presentation	Annually	All staff	MLRO
Log	AML Staff Training Log	Periodic	MLRO	MLRO

8.5 Anti-Bribery & Corruption Policy

The Company has embedded this Anti-Bribery & Corruption (ABC) Policy within the main AML Policy under this section. It outlines the commitment of Versus Odds B.V. to conducting its business activities in an ethical and lawful manner. The Company is dedicated to prevent bribery and corruption in all its operations and is committed to fostering a culture of integrity, transparency, and compliance.

The Company prohibits all forms of bribery and corruption, whether direct or indirect, and expects its employees, associates, contractors, and business partners to adhere to the highest standards of integrity and ethical behavior. This part of the policy applies to all employees, contractors, agents, suppliers, partners, and any individual or entity associated with the Company's operations, regardless of their role or position.

Definitions

Bribery: The offering, giving, receiving, or soliciting of any item of value (including but not limited to money, gifts, favors, entertainment, or services) to influence the actions of an individual in a position of trust or authority.

Corruption: The abuse of power or authority for personal gain, often involving bribery, embezzlement, fraud, or other unethical practices.

Associated Persons: Any individual or entity that has a business relationship with the Company, including employees, contractors, agents, suppliers, partners, and third-party intermediaries.

Prohibited Conduct

a. Bribery and Corruption: No employee or associated person shall engage in any form of bribery, corruption, or unethical behavior. This includes offering, promising, giving, receiving, or soliciting bribes or other improper benefits.

b. Gifts and Hospitality: Employees and associated persons must not offer or accept gifts, hospitality, or entertainment that could be seen as an attempt to influence business decisions or compromise the recipient's judgment.

c. Facilitation Payments: Facilitation payments (small unofficial payments to expedite routine processes) are strictly prohibited. Employees and associated persons must not make or accept such payments.

The Company is committed to conduct thorough due diligence on all third parties before entering into business relationships with them. This includes assessing their integrity, reputation, and compliance with anti-bribery laws.

Violations of this policy will not be tolerated and may result in disciplinary action, up to and including termination of employment or business relationships. In severe cases, legal action may be pursued. This policy will be reviewed periodically to ensure its effectiveness and relevance. Any necessary updates will be made to reflect changes in laws, regulations, and the Company's operations.

9. The screening process

The screening of potential customers against sanctioned persons, against PEPs is carried out by Versus Odds B.V. via a 3rd party Provider, a holistic and seamless Customer Due Diligence software.

Sanctions and PEP screening result: on each possible match by selecting the entity result, positive hits.

To screen customers, the Company selects the screening icon and inserts the customer details requested. Once this is done, the Company will be presented with the possible results together with searches conducted via third party screening as well as targeted google searches.

In addition to the identification and verification procedures, external search checks will be performed on the customer through the 3rd party provider's platform. Selecting the search engine item link shall direct the Company to another screen providing the actual information found within that link.

The Company is obliged to undertake measures at law aimed at combating terrorism, terrorism financing and the financing of the proliferation of weapons of mass destruction. This includes obligations emanating from the National Interest (Enabling Powers) Act relating to sanctions screening, freezing of assets and reporting.

10.Sanctions Lists

10.1Guidance on Implementation

According to CGA regulations service providers must take into account available information including any (updated) lists that for the purposes of fulfilling the obligation imposed on subject persons to combat the funding of terrorism, subject persons should, inter alia, have a system in place which detects whether an applicant for business is subject to any financial sanctions issued by, amongst others:

- EU Sanctions List - https://www.sanctionsmap.eu/#/main;
- The listing of the Office of Foreign Assets Control (OFAC) - https://sanctionssearch.ofac.treas.gov/; and
- The UN Sanctions List - https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list.

Such system should be sufficiently adequate for subject persons to keep themselves updated with all sanctions that might have an impact on their business operations.

10.2 Policy

Sanctions list screening is the responsibility of the MLRO. The performance of the screening procedures may be delegated or outsourced.

In obtaining, applying, and disseminating government and FATF findings, the MLRO ensures that all customers and business partners (e.g. Distributors) with whom a business relationship is established, are subject to due diligence procedures that ensure screening against relevant notices published by the OFAC, FIU and FATF.

Sanctions screening will form part of the initial due diligence procedures as well as the ongoing monitoring of customers and business partners as detailed in Annexes III and IV below. 'False positives' are investigated, and **any true sanction matches reported to the MLRO immediately.**

Staff are required to report where they have knowledge or a suspicion that financial sanctions measures have been or are being contravened.

10.3 Procedures and Documentation

All customers shall be subject to Sanctions screening once this is actively implemented as part of the initial due diligence procedures, with all customers being rechecked regularly as part of the ongoing monitoring of customers.

Staff responsible for performing Sanctions checks will receive specific training. Matches will be investigated by staff in order to identify true matches from those that are 'false positive'. All true sanctions matches must be reported to the MLRO immediately, using the Internal Unusual Transaction Reporting Form and followed up by an email thereafter.

11.Politically Exposed Persons

11.1Provisions from the NOIS

Article 5a of the NOIS states: "...where the applicant for business or the beneficial owner is subsequently found to be or becomes a politically exposed person, customer due diligence shall proceed in accordance with article 5b of the NOIS."

Appendix 1 of the P&G defines "politically exposed persons" as individuals who are or have been entrusted with promoting public functions, including heads of states or of governments, senior politicians, senior government, judicial or military officials, senior executives or publicly owned corporations and important political party officials.

11.2 Guidance on Implementation

In relation to PEPs the P&R indicates that service providers must have appropriate risk management in place to determine whether it's (proposed) clients are considered political exposed persons ("PEP's) and must conduct enhanced due diligence for PEPS, their families and associates. The service provider's decision to enter into business relationships with a PEP must be taken at its senior management level. The service provider must make reasonable efforts to ascertain that the PEPs source of wealth and source of funds/income is not from illegal activities and where appropriate review the customer's credit and character and the type of transactions the customer would typically conduct. Service providers must not accept or maintain a business relationship if the service provider knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial wonder is subsequently found to be, or subsequently becomes a PEP, institutions must obtain senior management's approval to continue the business relationship. Where the institution is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship.

11.3 Policy

It is Versus Odds B.V.'s policy not to accept PEPs as customers and the Company will proceed to end the relative business relationship with any individual/s found to be PEPs (notwithstanding declaring otherwise in the onboarding process).

Risk assessments for new customers, products or features will take account of the risk that the product might be used by PEPs for money laundering purposes.

11.4 Procedures and Documentation

A third-party check shall be carried out on each person to assess whether the person in question is a PEP.

Annex I – Compliance Officer / MLRO Job Description

MLRO

Responsibility

Versus Odds B.V. is responsible for appointing an MLRO of appropriate seniority with access to the resources required to effectively perform the role. Resources include time, support staff, the freedom and independence to act on authority, and access to relevant data / information.

In summary, the Board of the Company delegates the following high-level responsibilities to the MLRO:

- Establishing and operating appropriate risk-based internal policies, procedures and controls to prevent money laundering or terrorist financing, consistent with legal and regulatory requirements as set out in Curaçao and international provisions.
- Reviewing, updating and approving AML and CFT policies based on an assessment of risk and its management, ensuring that such assessments are kept up to date.
- Ensuring that priority is given to the implementation of AML and CFT policies and take ultimate responsibility for the development and operation of procedures that implement policy.
- Maintain up-to-date documentation detailing the risk-based AML and CFT arrangements operated by the Company.

MLRO Role

The MLRO may delegate certain functions, in particular those related to the day-to-day monitoring of procedures and systems to detect unusual activity, to suitable individuals in Versus Odds B.V. (where resources are available).

It is the MLRO's ultimate managerial responsibility to ensure that the provisions of this Policy are enforced. Where the MLRO delegates any activities, he will remain accountable for the operation of the delegated functions.

The MLRO may hold other senior management responsibilities within entities of Versus Odds B.V., to the extent that they do not interfere with their ability to conduct the MLRO duties.

In the absence of the MLRO for a period of less than 12 weeks, the MLRO duties will be temporarily performed by a suitably experienced and qualified individual from within Versus Odds B.V. The MLRO will always remain reachable and in close contact with the head office.

Should the position of the MLRO become vacant (i.e. the MLRO be absent for a period of 12 weeks or more in a consecutive 12-month period), the Board will appoint another suitably-qualified individual as its MLRO.

POSITION RESPONSIBILITIES

Establishing and supervising AML and CFT systems and controls
Developing and overseeing the implementation of appropriate **AML and CFT policies and procedures.** Determining the level of **resources** required to execute appropriate AML and CFT policies and procedures. Maintaining and developing the **risk-based approach** to AML and CFT arrangements **-** carrying out regular **assessments** of the adequacy of systems and controls. Reviewing the output from the **unusual activity monitoring** processes. Ensuring that AML and CFT requirements are considered as **part of the development** of new products, or service changes. Obtaining Board approval for significant **process changes.** Ensure that policies and procedures are accurately documented in the **AML Policy** which should be available to staff and used to guide training. Ensure that the Board are kept informed of the **money laundering risks** posed by the business and its activities, and how these are managed and mitigated. Reporting to the Board on a regular basis detailing the operation and effectiveness of the systems and controls used to combat financial crime. Documenting and ensuring that any actions recommended by the Board are **implemented**. Arranging and assisting with **regulatory visits** and **audit inspections.**

Maintaining relevance of the AML systems
Regularly reviewing developments in applicable **legislation and guidance** (domestic and international where the business is involved). Ensuring that **policies and AML are updated** to meet changing regulatory and business requirements. Ensuring that the operation of systems and controls are **monitored** and that they implement policy. Ensuring that relevant staff are provided with **training** appropriate for their position (frequency and content) and that all new staff receive training within the specified period. Ensure that **training materials** remain up-to-date and relevant to the business.

Reporting unusual activity
Investigating **internal Unusual Transaction Reports (UTRs)**. Deciding, following investigation, whether the internal report gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion and submitting an **external UTR to the Curaçao Financial Intelligence Unit (FIU)** where appropriate. **Documenting the reasons** for not submitting an external UTR to FIU and/ where an internal report has been made, considered and deemed not to be suspicious. Maintain a **filing system** of all internal UTRs, separating between those reported to FIU and those not.Ensure that relevant **records are retained** for the prescribed periods. Where required be the main **point of contact** for law enforcement officials.

Annex II – Risk Mitigation Matrix and Risk Factors

Risk Assessment and Mitigation Matrix

Risk Number	Risk Identification	Current mitigating controls	Residual risk as a result of mitigations	Comments
R001	High, or no transaction or transfer limits may be linked to money laundering;	Application of transaction limits on individual transactions (See Annex VI). In addition, payments originate only from bank accounts (no cash)	Medium	None
R002	Frequent cross-border transactions can give rise to difficulties with information sharing;	All cross-border transactions originate only from bank accounts (no cash). High Risk Jurisdictions are also subject to enhanced due diligence (see Annex III below)	Low	None
R003	Some betting, gaming activity pose a higher risk of money laundering. This is because of the higher amounts of funds that are transacted and because of the opportunities presented within that environment;	All cross-border transactions originate only from bank accounts (no cash). High Risk Jurisdictions are also subject to enhanced due diligence (see Annex III below)	Medium	None

R004	Transfers by unverified parties presents a higher risk of money laundering, whether it is the customer who is unverified or a third party;	Details on the customer (including bank account, name and surname) are received from the bank from which bank transfers originate	Low	None
R005	Transfers using cash offers little or no audit trail of the source of the funds and hence presents a higher risk of money laundering;	All transactions to and/or from Clients are by bank account (or authorized payment institutions)	Low	Cash is not accepted
R006	The non face-to-face nature may give rise to increased risk, such as impersonation fraud;	Application of Customer Due Diligence verification to non face-to-face customers (see Annex III)	Low	None
R007	Increased product functionality may in some instances give rise to higher risk of money laundering (product functionality includes person-to business, person-to-person, and business-to-business transfers);	Clients are all individuals and therefore there is limited product functionality	Low	None

R008	Products that feature multiple cards linked to the same account increase the utility provided to the user, but may also increase the risk of money laundering, particularly where the customer is able to pass on linked 'partner' cards to anonymous third parties;	All transactions to and/or from Clients are by bank account (or authorized financial institutions)	Low	Transactions by same customer with multiple cards are analyzed and copies of cards are requested.
R009	Segmentation of the business value chain, including use of multiple agents and outsourcing, in particular to overseas locations, may give rise to a higher risk;	All transactions to and/or from Clients are by bank account (or authorized financial institutions)	Low	No agents and limited outsourcing.
R010	Transfer of funds from or to countries with high levels of organized crime or drug production/distribution.	IP blocking is applied	Medium	None
R011	Making funds available to persons subject to financial sanctions.	Sanction checks shall be carried out on Clients as part of onboarding procedures and ongoing monitoring	Low	None

R012	Customers who are in a public position and/or location which carries a risk of exposure to the possibility of corruption.	PEPs shall be identified via third party database. Application of Enhanced Due Diligence to PEPs including requirement to provide source of wealth and funds.	Low	None
R013	Transmission of money from or to individuals, organizations or locations that may be linked to terrorist activity.	Application of transaction limits on individual transactions (See Annex VI). Payments originate only from bank accounts or authorized financial institutions (no cash). Also, CDD measures and noting of commercial activity.	Low	

Risk Factors Table

The below represented risk factors relevant to Versus Odds B.V.'s current service offerings that could indicate Money Laundering or Funding of Terrorism as per the risks highlighted in the table above.

Risk Factor	Risk Factor	Risk score	Mitigating Reasons
Customer	PEP/Sanctioned	10	None
Customer	Customers based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime or drug production/distribution	10	None
Geographical Area	Merchant's customers are based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime or drug production/distribution	10	None

Process for Determining Customer Risk (to be implemented)

The activities of each customer, the product, the distribution channels and the geographic area are assessed in relation to the risk factors above and the said assessment is recorded. A proposed risk assessment of Low, Medium or High is recorded whereby a low risk assessment is awarded to a customer with a 0-3 risk score, a medium risk assessment to a customer with a 4-7 risk score and a high-risk assessment to a customer with 8-10 risk score.

Members of staff may take into account any applicable mitigation reasons set out in the table above, in which case the reasons for the mitigation are recorded. The risk assessment may be revised on the basis of these mitigations subject to the consideration that a risk may never be assessed as low where:

i. the client is non-face-to-face (save for those instances detailed in the section entitled "Simplified Due Diligence" a) or b))
ii. the client is a PEP
iii. the client is from or is active in a high-risk jurisdiction

Annex III – Customer Due Diligence

The Company has established systematic procedures for identifying an applicant for business and ensuring that such identity is verified on the basis of documents, data or information obtained from a reliable and independent source.

Persons subject to Identification and Verification

For the purposes of the gaming services provided the follow legal and/or natural persons shall be subject to identification and verification procedures as stipulated below.

i. The Player being the natural person who is registered with the Company to which online gambling services are provided by the Company;
ii. A company or legal entity which is considered to be an intermediary of the Company to which online gambling services are provided by the Company;
iii. The Ultimate Beneficial Owners of a Company or legal entity which is considered to be an intermediary of the Company;
iv. The Directors of a Company or legal entity which is considered to be an intermediary of the Company;

For the purposes of the above that the "**ultimate beneficial owner**" of a body corporate or a body of persons includes all natural persons who ultimately own or control, whether through direct or indirect ownership or control, 25% or more of the shares or voting rights in the Company or legal entity in relation to which services are or will be provided.

Provided that natural persons who ultimately own or control a company that is listed on a regulated market which is subject to disclosure requirements consistent with Community legislation or equivalent international standards shall be excluded from verification requirements.

Provided further that in the case of a trust where beneficiaries have not been determined, due diligence will be carried out on any class of persons in whose main interest the trust is set up.

For the purposes of the above that the "**beneficial owner**" of a body corporate or a body of persons includes all legal persons who own or control, whether through direct or indirect ownership or control, 25% or more of the shares or voting rights in the Company or legal entity in relation to which services are or will be provided,

Provided that companies that are listed on a regulated market or otherwise subject to financial business regulation which are subject to disclosure requirements consistent with Community legislation or equivalent international standards shall be excluded from verification requirements. In such a case Simplified Due Diligence should be followed for Client On-boarding.

Provided that for Directors, the Company shall only be required to identify such persons and hence, notwithstanding anything to the contrary, no verification shall be required to be collected.

Organogram

In order to be able to identify each of the persons subject to identification and verification as part of the on-boarding process, the applicant for business is to provide an up-to-date organogram to the Company which is to be signed by an authorized official of the applicant, both at on-boarding and each time that there is a significant change in ownership.

Due Diligence for Natural Persons

Where the persons subject to identification and verification are natural persons, the following information shall be obtained in all cases in relation to identification and verification:

OPTION A:

1. Verification of Details - one of the following:
 1.1. a valid unexpired passport; or
 1.2. a valid unexpired national or other government-issued identity card; or
 1.3. a valid unexpired driving license.
2. Verification of Residential Address - one of the following not older than six (6) months:
 2.1. a recent statement from a recognized credit institution;
 2.2. a recent utility bill;
 2.3. correspondence from a central or local government authority, department or agency;
 2.4. any government-issued document where a clear indication of residential address is provided; or
 2.5. any other document as may be issued by the FIU.

In addition to the above, one of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**Medium Risk'** and two of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**High Risk'** as follows:

OPTION 1: One of the following

1. a professional reference (warranted lawyer or auditor)
2. a bank reference
3. an additional recent statement from a recognized credit institution;
4. an additional recent utility bill;
5. correspondence from a central or local government authority, department or agency;
6. any government-issued document where a clear indication of residential address is provided; or
7. any other document as may be issued by the FIU.

OPTION 2:

1. *The first payment be made from a bank set up in the EU or of a reputable jurisdiction with similar standards of banking regulation. For the purposes of this option 'bank' may also include financial institution, payment institution or electronic money institution.*

OPTION 3:

1. *Determination of source of wealth and source of funds signed by a recognized accountant/auditor.*

OPTION 4:

1. *Police conduct certificate*

OPTION 5:
Require that the documentation provided in OPTION A.2 and A.3 above is certified by a legal professional, accountancy professional, notary, person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction. Such certification should be evidenced by a written statement stating that:

- the document is a true copy of the original document;
- the document has been seen and verified by the certifier; and
- the photo is a true likeness of the applicant for business or the beneficial owner, as the case may be.

  The certifier must sign and date the copy document (indicating his name clearly) and clearly indicate his profession, designation or capacity on it and provide his contact details.

Provided that in all cases where the applicant, beneficiary owner or the ultimate beneficial owner is a PEP, Versus Odds B.V. will proceed to end the relative business relationship.

Due Diligence for Legal Persons
Part A

Where the persons subject to identification and verification are legal persons the following information shall be obtained in all cases in relation to identification and verification:

a) to identify the following:
i) the legal person's official full name;
ii) the legal person's registration number (if applicable);
iii) the legal person's date of incorporation or registration; and
iv) the legal person's registered address or principal place of business.

b) To verify the information and legal status mentioned under Part A(a), the most recently dated version of any of the following documents must be obtained:
i) Memorandum and Articles of Association; or
ii) Certificate of Incorporation; or
iii) Signed declaration by an authorized official of the applicant for business; or
iv) Company registry search, which includes confirmation that the private company has not been, and is not in the process of being dissolved, struck off, wound up or

terminated; or

v) Latest annual return; or

vi) Other statutory document.

In relation to the above, the staff member must view the original document, a certified copy of the original or a downloaded copy from the official registry website. Certification should be carried out by the company secretary, a director or an officer occupying an equivalent position or by the Registrar of Companies or a person occupying an equivalent position in a foreign jurisdiction.

Alternatively, certification may be carried out by a legal professional, accountancy professional, notary, person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.

The certifier must sign and date the copy document (indicating his name clearly) and clearly indicate his profession, designation or capacity on it and provide his contact details.

The certified copy of the original or the copy downloaded from the official registry website shall be retained by Versus Odds B.V. Where an original document is viewed, Versus Odds B.V. shall keep a true copy of the document, signed and dated by an officer of the subject person, on file.

Alternatively, identification and verification may be carried out by obtaining one or more additional (different) documents from amongst the list provided in Part A (b) above which verify the information obtained through the first set of documentation provided.

In addition to the above, one of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**Medium Risk'** and two of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Customer's risk has been assessed as '**High Risk'** as follows:

OPTION I:

1. Latest audited financial statements; provided that in case of Enhanced Due Diligence, this shall only be required if allowed by the jurisdiction of the applicant for business.

OPTION II:

1. The first payment be made from a bank set up in the EU or in any other jurisdiction with similar standards of banking regulation. For the purposes of this option 'bank' may also include financial institution, payment institution or electronic money institution.

OPTION III:

1. Certificate of good standing or a certificate of incumbency, not older than six (6) months.

OPTION IV:

1. A professional reference signed and duly dated by a legal professional, accountancy professional or notary.

Part B

Post identification and verification of the Legal Person, the Company shall also identify all the directors. This shall be done by either of the following:

i) referring to the list of directors contained in the most recent version of the Memorandum and Articles of Association; or
ii) by performing a company registry search provided that the officers of the company are listed therein; or
iii) by obtaining a copy of the directors' register of the company.

Part C

Upon the identification of the shareholders and Ultimate Beneficiary Owners' details as a result of the Organogram and documentation provided as mentioned above, the staff member shall perform and record the Due Diligence provided for natural persons in respect of such Ultimate Beneficiary Owners with particular regard to non-face-to-face procedures if required:

Provided that should the applicant's operations be regarded as high risk, shareholders having between 10% but less than 25% of the control in the applicant, may be required to provide for identification details including but not limited to First Name, Last Name and Date of Birth.

In instances where the documentation provided under Part A(b) does not identify the shareholders and the Ultimate Beneficiary Owners, the applicant for business has to supply any of the following documents:

i) Latest share register; or
ii) Signed declaration by an authorized representative of the applicant for business, which declaration should include sufficient details to enable the subject person to identify the shareholders and the Ultimate Beneficiary Owners.

For avoidance of doubt, no proof of address will be requested of shareholders holding an interest between 10%, but less than 25%.

Languages

All documents are to be provided in English (or any other language which any official of the Company understands). Certified translations are to be translated of documents in other languages.

Client Terms and Conditions

The Client Terms and Conditions includes a declaration by an authorized representative of the applicant for business as to whether they have:

a) ever been convicted of an offence (other than a minor traffic offence);
b) ever been adjudged bankrupt;
c) ever been the subject of an investigation by a government, professional or other

regulatory body;

d) ever been a director, shareholder, officer or manager of a business entity which has been the subject of an investigation as aforesaid
e) ever been a director, shareholder, officer or manager of a business entity which has been adjudged bankrupt compulsorily would up or has made any compromise or arrangement where its creditors or has otherwise ceased trading in circumstances where its creditors did not receive or have not yet received full settlement of their claims; and
f) unless otherwise disclosed in the terms and conditions, ever had or currently has any direct or indirect beneficial interest in or whether he ever was or currently is a director of any other company registered in Curaçao.

Customer Risk Assessment

Each customer is subject to a risk assessment and subsequently rated as Low Risk, Medium Risk or High Risk as set out in Annex II above.

For the purposes of such assessments additional information may be required from the customer.

Face-To-Face Transactions or Clients

In all instances of face-to-face onboarding, provided that the applicant does not provide certified true hardcopies or the originals of the documentations required as per the abovementioned procedures, the Company representative is to view the original document, make a hard copy of such document (printed scan/photograph etc.) and certify that this is a true copy of the original seen by him, while duly signing the document including the relevant date.

All instances of face-to-face clients will require any one of the following:

a) Include an email on file confirming that a face-to-face meeting with the applicant for business duly occurred prior to onboarding;
b) A certified true copy in original by a Versus Odds B.V.'s representative of an identification document of the applicant for business' representative, provided that such document was copied (scanned, photographed etc.) by a Company's representative himself; or
c) Minutes of the meeting with the applicant for business' representative, signed and duly dated by the Company representative.

Timing of Due Diligence

Each client shall provide a copy of all documentation in order to assess that all the documentation is in order upon the first withdrawal and/or upon the sum of Naf 4,000 (Eur 2,000) with accumulative withdrawal threshold reached by the player.

In some instances, a corporate client (intermediary) may select to sign the Services Agreement prior to the carrying out of on-boarding to provide a commitment to eventual onboarding. In this case, no services are permitted, and no services shall be provided to the client and no transactions entered into prior to the carrying out of all due diligence procedures and prior to on-boarding.

In the event that due diligence documentation is not provided within thirty (30) days from the initial request by the Company or it otherwise becomes obvious that the client is not able to satisfy due diligence requirements, the Service Agreement or player registration shall be terminated. The MLRO will consider the appropriateness of filing an UTR.

Annex IV – Client Acceptance Policy

The Companies or intermediary of the Company policy for acceptance of customers takes into consideration the Risk Assessment and Mitigation measures as well as the Risk Factors indicated in Annex II above.

Client Acceptance

The Company or an intermediary of the Company shall not accept the following clients:

i. Clients that fail the relevant due diligence identification and verification controls set out in Annex III above;
ii. Clients who themselves or their ultimate beneficial owners are excluded customers listed below;
iii. Clients who have in the past been reasonably associated or involved in criminal activities or other illegal activities may result from searches on the clients, beneficial owners and on any other person in relation to whom due diligence is carried out.

Excluded Activities

The Company or its intermediaries shall not accept the following types of business activities for any provision of services:

i. Trading in Arms
ii. Supplying Technology or Parts Connected with Defense
iii. Providing Military Security Services
iv. Clients resident in jurisdictions where the Company - or its affiliated Group Companies with whom service agreements are in place - are not authorized to provide gaming services.

Excluded Individuals

The Company or its intermediaries shall not accept the following persons:

i. Sanctioned Individuals and/or entities;
ii. Entities with bearer shares;
iii. Entities where UBOs cannot be identified;
iv. Persons who seek to set up a business relationship or conduct an occasional transaction in the name of third parties under an anonymous name or nickname;
v. Customers having underlying customers

Risk-Based Approach for Accepting Clients

On the basis of the risk approach highlighted in Section 3 of the AML Policy and Annex II above, risk factors are taken into account to determine the risk of each customer (low, medium or high). Different levels of Enhanced Due Diligence are applied in the event of Medium or High-risk assessments.

The manner in which the assessment is carried out is highlighted in Annex II above.

Annex V – Internal UTR Form

Internal UTR Form Template

The UTR should be a prompt report and escalated to the FIU as soon as practically possible.

(Please send the Internal UTRs to the Compliance Officer / MLRO and cc the Deputy MLRO if exist)

A record of this UTR together with all related documents will be kept by the Compliance Officer / MLRO for at least five (5) years.

Reporter's details (this section is to be completed by the Reporter)	
Reporter's name:	
Reporter's email:	
Date:	
Department:	

Individual subject(s) of the SAR (this section is to be completed by the Reporter)	
Customer's user ID/username/brand:	
Relationship start & end date:	
Customer's full name:	
Customer's residential address:	
Customer's date of birth:	
Customer's phone number(s):	
Customer's email address:	
Customer's gender:	
Customer's nationality:	
Linked account(s):	
What is the reason for reporting?	
Multiple Accounts?	Y/N
Use of Multiple IP Address via Proxies/VPNs to Mask Location and/or Identity?	Y/N
Suspected Account Hijacking?	Y/N
Unusual Gaming / Account Activity?	Y/N
Bonus Abuse?	Y/N
Fraudulent Refund Request?	Y/N
Non-Compliance with Requests?	Y/N
Other (please specify)	
What evidence is supporting your suspicion? *(Please add sources & links such as: transaction records, chat logs, email correspondence, account activity logs, screenshots, etc.).*	

Aggregate lifetime deposits (across brands):	
Aggregate lifetime withdrawals (across brands):	
Balance (including pending WDs) in account at UTR reporting date (across brands):	
AML details (this section is to be completed by the Reporter)	
ID Reference Number:	
ID Expiry Date:	
Known occupation:	
CDD / EDD Status:	
Status of business relationship:	
Services utilized:	
Reference nr. if linked to a previous UTR:	

Activity Information (this section is to be completed by the Reporter)
Provide a comprehensive description of the suspicious activity, including dates, times, and any relevant transactions or behaviors observed. Please also provide an overall total of deposit/withdrawal amount for each payment method, including the first and last date of each payment method used. *It may be easier to export this as an excel document and attach.*

Supporting documentation attached (this section is to be completed by the Reporter) *When you escalate the internal UTR please attach in the email: ID, Proof of address documents, deposit history (excel sheet), withdrawal history (excel sheet), login history (IP address on excel sheet), chat logs, email correspondence, account activity logs, screenshots, etc.*	
Customer Due Diligence Documents (ID / UB):	Customer Notes:
List the IP addresses customer used to log on:	Customer Communications Logs:
Value and volume of withdrawals and deposits:	Payment Gateway Information related to customer:

Timeline of the Suspicious Activity (this section is to be completed by the MLRO)

(The timeline should be detailed and sufficiently clear that someone not familiar with the activity or Company would understand it. Please avoid jargons and acronyms) xx/xx/xxxx – Customer opened his/her xx account xx/xx/xxxx – We verified ID, Proof of address, etc. xx/xx/xxxx – We found a negative adverse media regarding our player (*include link if available, date and a short summary about the article*) xx/xx/xxxx – Account was closed. xx/xx/xxxx – An internal SAR was considered.
The information or other matter which gives the grounds for your knowledge, suspicion, or belief: - Negative adverse media have found; - Possible problem gambling signs; - No cooperation with our Due Diligence Documentation / Source of Wealth request. - No cooperation with our Customer Support / Risk, Payments & Fraud Team.

MLRO Determination (this section is to be completed by the MLRO)
3. Did we find positive info online on the player that would discharge our concerns? 4. Did we find any negative info found online or in the account history, data, behavior, documents etc, that would mean we clearly need to report? ***Should the answers to be no for both of these, we must consider:*** ● The country is x AML risk according to FATF, ● Payment method is x risk (visa, bank, etc.), ● spend is x risk. I suggest we file this as a SAR, but that will depend on the answers above.

Annex VI – Business Risk Assessment

In accordance with regulatory expectations set forth by the Curaçao Gaming Authority, the Company has conducted a comprehensive Business Risk Assessment addressing all relevant operational, compliance, and financial risk factors.

Due to the scope, length, and level of detail required to meet these regulatory standards, the full Business Risk Assessment has been compiled as a standalone document. This allows for a thorough review of identified risks, control measures, and the Company's ongoing risk mitigation strategies.

In short, the Business Risk Assessment of the Company includes:

- an introduction of Versus Odds B.V.;
- identification and scoring of inherent risks;
- determination of risk appetite;
- analysis of AML/CFT controls;
- determination of residual risks;
- remediation plan;
- conclusion; and
- an appendix for weighing and scoring.

For complete information, please refer to the separate document titled "Business Risk Assessment – Versus Odds B.V.".

Annex VII – Abbreviations

AML	Anti-Money Laundering
AML Regulation	Regulations Concerning Anti-Money Laundering and Countering Terrorism Financing
CMP	Compliance Monitoring Program
CFT	Combating Funding of Terrorism
EU	European Union
KYC	Know Your Customer
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
TF	Terrorist Financing
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
RBA	Risk Based Approach
UTR	Unusual Transaction Report

Annex VIII – Signatory page

Versus Odds B.V.
Curacao, 19th May 2025

Signed by:

8737E2B30CF043F...

Analissa Mercedes Eustatius Heiland
Xecutive Corporate Management B.V. – Managing Director

Signed by:

E9C1A4A3F74E4ED...

Lorenza Godett
Xecutive Corporate Management B.V. – Managing Director

Signed by:

C844330A35F54B6...

Mark Cauchi
Key Compliance Officer