

AML Policy

Copyright information

This document is the exclusive property of Viral Technology N.V., 2025. The recipients agree that they may not copy, transmit, use, or disclose the confidential and proprietary information in this document by any means without the expressed and written consent of Viral. By accepting a copy, the recipient agrees to adhere to these confidentiality conditions.

© All rights reserved Viral Technology N.V., 2025

Document information			
Document name:	AML Policy	Document ID:	
Document version:	3.0	Date of approval:	2025-05-27
Approved by:	Christoph Härtel	Revision interval:	Annual
Document owner:	Alessandro De Luca	Information classification :	Internal information , no personal data
Reference :	https://www.gamingcontrolcuracao.org/regulation/aml	Internal reference:	
Revision history			
Author:	Version:	Date:	Change history:
Sari Aitokallio	1.0	2024-06-18	Existing version transferred from Sharepoint to Confluence
Christoph Hartel	1.0	2024-06-19	Policy transfer approved

Sari Aitokallio	2.0	2024-08-28	Policy updated in line with the new Curacao AML policy from September 2024
Christoph Hartel	2.0	2024-08-28	Version 2.0 approved
Alessandro De Luca	3.0	2025-05-23	Policy updated (clauses 3.Audience and 4. Definitions added, BRA, CRA, CAP, CDD introduced as a separated clauses) in line with the new Curacao AML policy from January 2025
Christoph Hartel	3.0	2025-05-27	Version 3.0 approved

- [1. Policy Statement](#)
- [2. Purpose](#)
- [3. Audience](#)
- [4. Definitions](#)
- [5. Business Risk Assessment \(BRA\) Implementation](#)
 - [5.1 Business Risk Assessment \(BRA\) schedule and areas](#)
 - [5.1.1 AML and GDPR risks](#)
 - [5.1.2 Information security risks](#)
 - [5.1.3 Technology risks](#)
 - [5.1.4 Operational risks](#)

- [5.1.5 Commercial risks](#)
 - [5.1.6 Legal risks](#)
 - [5.1.7 Financial risks](#)
- [5.2 Scope, Context, and Criteria:](#)
 - [5.2.1 Risk Identification:](#)
 - [5.2.2 Risk Analysis:](#)
 - [5.2.3 Risk Evaluation:](#)
 - [5.2.4 Risk Treatment:](#)
 - [5.2.5 Communication and consultation](#)
 - [5.2.6 Monitoring and Review:](#)
- [5.3 Assessing risks](#)
 - [5.3.1 Assessing risks in money-laundering and terrorism financing](#)
 - [5.3.2 Assessing technology / information security related risks](#)
 - [5.3.3 Assessing Operational and Commercial Risks](#)
 - [5.3.4 Assessing Legal Risks](#)
 - [5.3.5 Assessing Financial Risks](#)
- [5.4 Calculating inherent risk level](#)
- [Risk Assessment Matrix:](#)
- [5.5 Calculating residual risk](#)
- [5.6 Guidelines for management actions](#)
- [5.7 Follow-up and reporting](#)
- [6. Customer Risk Assessment \(CRA\) implementation](#)
 - [6.1 Description of customer risk assessment process](#)
 - [6.2 Risk assessment schedule and teams](#)
 - [6.3 Scope, Context, and Criteria](#)
 - [6.4. Calculating inherent risk level](#)
 - [Risk Assessment Matrix:](#)
 - [6.6 Calculating residual risk](#)
 - [6.7 Guidelines for management actions](#)
- [7. Customer Acceptance Policy \(CAP\)](#)
 - [7.1. General principles](#)
 - [7.2. Minimum Information Required for Acceptance](#)
 - [7.3 Acceptance Categories Based on CRA Risk Levels](#)
 - [7.3 Contractual AML Obligations](#)
- [8. Customer Due Diligence \(CDD\)](#)
 - [8.1 Overview and Objectives](#)
 - [8.2 Due Diligence Frequency](#)
 - [8.3 CDD Measures](#)
 - [8.4 Know Your Business \(KYB\)](#)
 - [8.5 Know Your Customer \(KYC\)](#)
 - [8.6 Know Your Supplier \(KYS\)](#)
 - [8.7 Politically Exposed Person \(PEP\) Screening](#)
 - [8.8 Manual Screening & Adverse Media Checks](#)
 - [8.9 Enhanced Due Diligence \(EDD\)](#)
 - [8.10 Recording Due Diligence Results](#)
 - [8.11 Ongoing Monitoring](#)

- [8.12 Reliance on Third Parties for CDD](#)
 - [8.13 Record Keeping](#)
- [9. Reporting of Unusual Transactions](#)
- [10. Anti-Money Laundering Compliance Program](#)
- [11. Obligations towards B2C operators](#)
- [12. Training Programs](#)
- [13. Compliance and Consequences of Non-Compliance](#)
- [14. Related Information](#)
- [15. Contact Information](#)

1. Policy Statement

Viral Technology N.V (hereinafter Company)., reg No. 123604, having its registered address at Groot Kwartierweg 10, Livestrong Building, Curaçao have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity. This policy applies to the identification and verification of our business partners and aims to ensure compliance with applicable local and international laws. No Player Data will be sold or given or shared with any person or corporation.

2. Purpose

It is the policy of Viral Technology N.V (the "Company") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions in which the Company operates, to prevent of the use of the financial system for the purpose of money laundering and terrorist financing.

The Company is fully committed to prevent money laundering and combat the financing of terrorism in order to minimize and manage risks such as the risks to its reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.

The Company will endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation from the threat of money laundering, the funding of terrorist and other criminal activities.

The Company's policies, procedures and internal controls are designed to ensure compliance with all applicable laws, rules, directives and regulations relevant to the Company's operations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

3. Audience

This policy applies to:

- All employees,
- Company management
- Third-party contractors engaged in onboarding or compliance operations.

4. Definitions

Key terms relevant to this policy:

- MLRO - Money Laundering Reporting Officer
- BRA - Business Risk Assessment
- CRA - Customer Risk Assessment
- DD - Due Diligence
- EDD - Enhanced Due Diligence
- CAP - Customer Acceptance Policy
- PEP - Politically Exposed Person
- ML - Money Laundering
- TF - Terroris Financing
- CDD - Customer Due Diligence
- KYC - Know Your Customer
- KYS - Know Your Supplier
- KYB - Know Your Business
- FIU - Financial Intelligence Unit Curaçao
- Game Content - third party produced casino games
- Player - End user on B2C websites (not a direct customer of the Company)

5. Business Risk Assessment (BRA) Implementation

5.1 Business Risk Assessment (BRA) schedule and areas

Risk assessment is performed annually by the functional risk areas, and reported to the CEO.

The assessment is divided into areas:

5.1.1 AML and GDPR risks

The Anti-Money Laundering/Countering of Financing of Terrorism risks are assessed by the Compliance function. The responsible for the update is the Head of Compliance. Risks related to game integrations, financial sanctions circumvention and geography are assessed.

The Data Protection risks are also assessed by the Head of Compliance team.

5.1.2 Information security risks

The risks related to information security are assessed by the CTO and the members of the development team together with the CEO.

5.1.3 Technology risks

The risks of the technology – game aggregation platform - are assessed by the CTO together with the members of the development team and the CEO.

5.1.4 Operational risks

Operational risks are assessed in the management team, and the responsible for the update is the CEO. Operational risks include the risks of erroneous or faulty operational processes in game integrations, technology development or administrative function. It also includes errors and fraud made by the Company's personnel out of incompetence, lack of training or intentional wrongdoing.

5.1.5 Commercial risks

Commercial risks include risks originating from business relationships, competitor behavior, customers, partners and suppliers. The responsible manager to assess the commercial risks is the CEO.

5.1.6 Legal risks

Risks originating from judicial environment and regulation are assessed by the Legal Counsel / Managing Director.

5.1.7 Financial risks

The financial risks include the risks to revenue, costs, expenses and the funding of the company. The risks are assessed by the CEO and Head of Finance.

5.2 Scope, Context, and Criteria:

Before commencing risk assessment, it's pivotal to define the scope, establish the context, and set the criteria of the risk assessment. This involves understanding the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the risk assessment process.

5.2.1 Risk Identification:

This step involves recognizing where, when, how, and why the events could occur that might jeopardize the achievement of objectives. This is crucial for identifying the causes and sources of risks and understanding the consequences and their impact on objectives.

When identifying possible risks, at least the following sources should be considered:

Sources of information	Approach to identifying risks
Analysis of actual security breaches, other security related threats	Annual/semi-annual and quarterly risk assessment/review meetings Strategy meetings Annual planning meetings Analyse of other jurisdictions on problematic patterns Stakeholder analysis Process analysis
Media	
Complaints reports	
Incident reports	
Analysis of customer feedback	
Claims data	
Team meetings	
Research reviews	
Financial data audits	

5.2.2 Risk Analysis:

Once risks are identified, they are then analyzed to understand their nature, sources, and consequences. This step involves determining the likelihood of the occurrence of the risk events and their impact or consequence, using either qualitative or quantitative methods, considering the range of possible outcomes, their probability, and their severity.

5.2.3 Risk Evaluation:

Post risk analysis, the risk evaluation process is undertaken to make decisions about the significance of risks. The evaluation compares the risk analysis results with the established risk criteria to determine where additional action is needed. This step helps in prioritizing the risks based on their potential impact and likelihood.

5.2.4 Risk Treatment:

Based on the risk evaluation, appropriate risk treatment options are developed and implemented to manage the risks. The options could include avoiding the risk, optimising the risk through mitigation strategies, transferring the risk, or accepting the risk, depending on the organisational context and risk appetite.

5.2.5 Communication and consultation

Communication and consultation is an essential attribute of good risk management. Risk management cannot be done in isolation and is fundamentally communicative and consultative. Hence this step is, in practice, a requirement within each element of the risk management process.

Formal risk reporting is only one form of risk communication. Good risk communication generally includes the following attributes:

- encourages stakeholder engagement and accountability
- maximises the information obtained to reduce uncertainty
- meets the reporting and assurance needs of stakeholders
- ensures that relevant expertise is drawn upon to inform each step of the process
- informs other entity processes such as corporate planning and resource allocation.

Different stakeholders will have different communication needs and expectations. Good risk communication is tailored to these requirements.

5.2.6 Monitoring and Review:

The risk assessment process also involves ongoing monitoring and review of the identified risks and the effectiveness of the risk treatment measures. The continual monitoring and review ensure that the risk management is dynamic, iterative, and responsive to change.

5.3 Assessing risks

5.3.1 Assessing risks in money-laundering and terrorism financing

The level of inherent risk refers to the general level of risk in the financial sector in response to money laundering or terrorist financing, with a view to the products and services provided by the company.

The following sources must be considered:

- National risk assessment, if publicly available
- Supranational risk assessment, such as FATF or EU
- EBA Risk Factors Guidelines
- FIU Curaçao AML/CFT reviews
- Best understanding of business trends and vulnerabilities in the gaming sector

5.3.2 Assessing technology / information security related risks

The Company is also a technology Company. The aggregation platform used in the Company's games integration is own technology, developed and maintained inhouse.

The information security is build in the technological solutions used in developing the game aggregation platform. The risks are related to the quality of coding, the interfaces to third parties and in the cybersecurity.

5.3.3 Assessing Operational and Commercial Risks

Operational and commercial risks are assessed based on the Company's business continuity, scalability, and exposure to customer-side failures. These include:

- Dependency on key personnel or single points of failure in operations;
- Reliability of third-party game content, integrations and uptime of the aggregation platform;
- Risk of customer insolvency, regulatory shutdowns, or reputational damage affecting commercial continuity;
- Business model alignment between the Company and its partners.

5.3.4 Assessing Legal Risks

Legal risks are assessed with regard to compliance with Curaçao laws, data protection rules, and cross-border contracting. This includes:

- Exposure to non-compliance due to lack of licensing in a partner's jurisdiction;
- Risks arising from international sanctions or AML laws;
- Contractual clarity around AML responsibilities, data use, and liability.

5.3.5 Assessing Financial Risks

Financial risks include exposure to delayed payments, high-risk payment flows, or unverified sources of customer funding. The Company evaluates:

- Payment terms, methods, and jurisdictions involved;
- Customer financial health indicators and adverse financial history;
- High-value contracts and refund or clawback risks.

5.4 Calculating inherent risk level

Inherent risk identifies the level of risk posed by a specific threat or hazard before the application of controls or mitigations. It is calculated using a combination of the **likelihood** of an event occurring and the potential **impact** should the event occur.

Likelihood represents the chance of a particular risk event occurring. It's a measure of the probability that a given risk will occur and can be expressed qualitatively (e.g., high, medium, low). Assessing likelihood involves considering various factors such as the frequency of occurrence, existing controls, and the vulnerability of the system or process.

Business Impact refers to the extent of damage or consequences that can occur if the risk eventuates. Business Impact assessed qualitatively (e.g., severe, moderate, minor) . When assessing impact, various aspects such as financial, reputational, operational, and compliance consequences need to be considered.

Likelihood scale		
Score	Scale	Likelihood
1	Very low	Very unlikely occurrence
2	Low	Slight likelihood of occurrence, possible once a year
3	Medium	Unlikely, may occur less than twice a year
4	High	Reasonable change of likeliness for a substantial number of times more than 3
5	Extreme	Will happen multiple times a year; very high occurrence
Business impact scale		
Score	Scale	Consequences
1	Minor	No or minimal damage
2	Low	The risk is unlikely to cause damage
3	Moderate	Moderate There is a slight chance of this risk causing some damage
4	High	High There is a considerable likelihood of this risk causing large damage.
5	Severe	Risk can cause a high and irreparable level of damage including substantial financial loss to the company

Risk Assessment Matrix:

In many risk assessment models under ISO standards, likelihood and impact are often used together in a two-dimensional matrix to determine inherent level of risk. The level of risk calculated as:

Inherent risk Level = Likelihood × Impact
--

- If both the likelihood and impact are high, the risk is typically considered critical and requires immediate attention and mitigation.
- If either the likelihood or impact is low, the risk may be considered less significant.

Likelihood * Impact scale					
Impact/Likelihood	1	2	3	4	5

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

5.5 Calculating residual risk

Residual risk is a remaining risk that exists after all risk mitigation measures, controls, and actions have been applied to reduce the inherent risk.

Score	Level of controls
5	Strong levels of controls. Risk mitigation procedures are fully functional and operational. Multiple measures in place. Residual risk: Negligible
4	Risk is managed adequately procedures are fully functional, yet detection may be bypassed, or manipulated such action is not easily done. Residual risk: Low to Medium
3	Risk is managed adequately, could be improved in certain parts, but works adequately and is effective. Residual risk: Medium
2	Risk is managed adequately, could be improved in certain parts, but works adequately and is effective. Residual risk: Medium to High
1	Risk mitigation present but ineffective OR does not address the area's of risk adequately, exposure to high risk and implementation is necessary OR there is no method of mitigating such risk OR Customer fails to provide relevant/requested information. Residual risk: High
Example of control levels	
5	Automated, system based controls
4	Partly manual controls, based on roles and training

3	Instructions in place, physical controls, audits
2	Policy in place
1	No controls

After identifying and assessing the strength of the mitigating controls, determine the residual risk, which is the remaining level of risk after the controls have been applied. This involves reassessing the likelihood and impact of the risk, considering the effectiveness of the controls.

Residual Risk = Inherent Risk– Level of controls					
Inherent risk - Level of controls					
Inherent risk/Control strength/	1	2	3	4	5
25	24	23	22	21	20
20	19	18	17	16	15
16	15	14	13	12	11
15	14	13	12	11	10
12	11	10	9	8	7
10	9	8	7	6	5
9	8	7	6	5	4
8	7	6	5	4	3
6	5	4	3	2	1
5	4	3	2	1	
4	2	2	1		
3	2	1			
2	1				
1					

5.6 Guidelines for management actions

Risk appetite matrix below, describes the Company risk acceptance and management actions based on identified risk level.

IF total residual risk score is identified as **Very Low** or **Low** - no action needed, risk acceptance is within risk appetite

IF total residual risk score is identified as **Medium** - risk is conditionally approved, risk mitigation controls should be applied within 30 day period **OR** risk is periodically monitored

IF total residual risk score is identified as **High** - risk is conditionally approved, risk mitigation controls should be applied within 7 day period **OR** risk is under constant monitoring

IF total residual risk score is identified as **Extreme** - such risk is not within the Company risk appetite, all operations related to this risk factors should be ceased, risk mitigation controls must be revised and applied immediately.

Risk tolerance matrix			
Total residual risk (risk score)	Impact	Acceptance	Management actions
Very low (1)	No or minimal damage - Risk will not manifest	Approved	No action needed
Low (2-5)	The risk is unlikely to cause damage - Less than once a year	Approved	No actions needed
Medium (6-11)	There is a slight chance of this risk causing some damage	Approved OR Conditional Approval: Insert additional control, action or mitigation	Improvement applied within 30 day period or periodical monitoring of risk
High (12-19)	There is a considerable likelihood of this risk causing large damage.	Conditional approval : Insert additional control, action or mitigation	Improvement applied within 7 days period OR constant monitoring of risk
Extreme (20-25)	Risk can cause a high and irreparable level of damage including substantial financial loss to the company	Decline	Stop operations immediately

5.7 Follow-up and reporting

The owner of a risk area will follow up the occurrence of risks, accidents, omissions or near-misses. The risk report to the CEO will include the medium to severe risk events and the actions to prevent reoccurrence. The minimum monetary value of the risks reported to the CEO is Euro 10,000 (damage or imminent damage).

6. Customer Risk Assessment (CRA) implementation

6.1 Description of customer risk assessment process

The Company conducts a Customer Risk Assessment (CRA) for each customer to identify, evaluate, and mitigate potential exposure to money laundering, terrorist financing, or proliferation financing risks associated with that customer relationship.

The CRA follows a risk-based approach, in line with international AML/CFT standards (e.g., FATF Recommendations), Curaçao Gaming Control Board (GCB) guidelines, and applicable EU directives. It uses a structured scoring system to assess the level of inherent customer risk and residual risk after applying mitigating controls.

CRA is conducted at onboarding and at least annually, or earlier if:

- There are material changes in ownership, jurisdiction, or business model;
- Adverse media or sanctions alerts arise;
- Unusual customer behavior or payment activity is detected.

6.2 Risk assessment schedule and teams

The CRA process is led by the Head of Compliance. The Head of Compliance is responsible for performing the initial and annual CRA reviews and reporting to CEO. Internal and external legal and financial professionals may assist in high-risk or complex cases.

6.3 Scope, Context, and Criteria

The CRA applies to all customer. The context includes geographic, regulatory, and financial exposure. The criteria are aligned with Curaçao AML obligations and FATF sectoral guidance for gaming businesses.

6.3.1 Risk Identification:

Each customer is evaluated across five key dimensions:

Risk Dimension	Description
Geographic Risk	Is the customer registered in or targeting high-risk jurisdictions per FATF or sanctions lists?
Regulatory Risk	Is the customer licensed in its operating jurisdiction or legally permitted to operate? Does it follow AML rules in lawless or grey jurisdictions?
Ownership Risk	Does the company have complex structures or unverified UBOs?
Reputational Risk	Has the company or its principals been involved in fraud, fines, or litigation?

Commercial Risk	Is the contract size unusually high or paired with non-transparent payment methods?
------------------------	---

Risk indicators are gathered using internal data, KYC/KYB documentation, and external screening tools.

6.4. Calculating inherent risk level

Inherent risk identifies the level of risk posed by a specific threat or hazard before the application of controls or mitigations. It is calculated using a combination of the **likelihood** of an event occurring and the potential **impact** should the event occur.

Likelihood represents the chance of a particular risk event occurring. It's a measure of the probability that a given risk will occur and can be expressed qualitatively (e.g., high, medium, low). Assessing likelihood involves considering various factors such as the frequency of occurrence, existing controls, and the vulnerability of the system or process.

Business Impact refers to the extent of damage or consequences that can occur if the risk eventuates. Business Impact assessed qualitatively (e.g., severe, moderate, minor) . When assessing impact, various aspects such as financial, reputational, operational, and compliance consequences need to be considered.

Likelihood scale		
Score	Scale	Likelihood
1	Very low	Very unlikely occurrence
2	Low	Slight likelihood of occurrence, possible once a year
3	Medium	unlikely, may occur less than twice a year
4	High	Reasonable change of likeliness for a substantial number of times more than 3
5	Extreme	Will happen multiple times a year; very high occurrence
Business impact scale		
Score	Scale	Consequences
1	Minor	No legal or regulatory consequence
2	Low	Internal issue, low chance of escalation
3	Moderate	Limited regulatory exposure or reputational concern
4	High	Likely to trigger regulatory scrutiny or fines
5	Severe	High regulatory exposure, sanctions, or media impact

Risk Assessment Matrix:

In many risk assessment models under ISO standards, likelihood and impact are often used together in a two-dimensional matrix to determine inherent level of risk. The level of risk calculated as:

$$\text{Inherent risk Level} = \text{Likelihood} \times \text{Impact}$$

- If both the likelihood and impact are high, the risk is typically considered critical and requires immediate attention and mitigation.
- If either the likelihood or impact is low, the risk may be considered less significant.

Likelihood * Impact scale					
Impact/Likelihood	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

6.6 Calculating residual risk

Residual risk is a remaining risk that exists after all risk mitigation measures, controls, and actions have been applied to reduce the inherent risk.

Score	Level of controls
5	Full CDD, sanctions/PEP screening, licensed customer, no adverse media Residual risk: Negligible
4	Valid documentation, minor gaps filled, no red flags Residual risk: Low to Medium
3	EDD applied, limited licensing, strong contract controls Residual risk: Medium

2	Some verification missing, complex structures, unclear funds Residual risk: Medium to High
1	No KYC or high exposure; onboarding blocked Residual risk: High
Example of control levels	
5	Automated, system based controls
4	Partly manual controls, based on roles and training
3	Instructions in place, physical controls, audits
2	Policy in place
1	No controls

After identifying and assessing the strength of the mitigating controls, determine the residual risk, which is the remaining level of risk after the controls have been applied. This involves reassessing the likelihood and impact of the risk, considering the effectiveness of the controls.

Residual Risk = Inherent Risk– Level of controls					
Inherent risk - Level of controls					
Inherent risk/Control strength	1	2	3	4	5
25	24	23	22	21	20
20	19	18	17	16	15
16	15	14	13	12	11
15	14	13	12	11	10
12	11	10	9	8	7
10	9	8	7	6	5
9	8	7	6	5	4
8	7	6	5	4	3
6	5	4	3	2	1
5	4	3	2	1	
4	2	2	1		
3	2	1			

2	1				
1					

6.7 Guidelines for management actions

Risk appetite matrix below, describes the Company risk acceptance and management actions based on identified risk level.

IF total residual risk score is identified as **Very Low** or **Low** - no action needed, risk acceptance is within risk appetite

IF total residual risk score is identified as **Medium** - risk is conditionally approved, risk mitigation controls should be applied within 30 day period **OR** risk is periodically monitored

IF total residual risk score is identified as **High** - risk is conditionally approved, risk mitigation controls should be applied within 7 day period **OR** risk is under constant monitoring

IF total residual risk score is identified as **Extreme** - such risk is not within the Company risk appetite, all operations related to this risk factors should be ceased, risk mitigation controls must be revised and applied immediately.

Risk tolerance matrix			
Total residual risk (risk score)	Impact	Acceptance	Management actions
Very low (1)	No or minimal damage - Risk will not manifest	Approved	No action needed
Low (2-5)	The risk is unlikely to cause damage - Less than once a year	Approved	Annual monitoring
Medium (6-11)	There is a slight chance of this risk causing some damage	Approved OR Conditional Approval: Insert additional control, action or mitigation	Enhanced controls, annual reviews
High (12-19)	There is a considerable likelihood of this risk causing large damage.	Conditional approval : Insert additional control, action or mitigation	Management approval required, quarterly monitoring

Extreme (20-25)	Risk can cause a high and irreparable level of damage including substantial financial loss to the company	Decline	Onboarding refused or terminated
-----------------	---	---------	----------------------------------

7. Customer Acceptance Policy (CAP)

7.1. General principles

The Customer Acceptance Policy defines the conditions under which Company accepts or rejects potential customers. It ensures that all customer relationships are entered into only after an appropriate risk-based assessment, in accordance with the Company's CRA, AML/CFT policies, and Curaçao regulations.

- The Company does not accept customers unless sufficient Know Your Customer (KYC) and due diligence documentation is provided and reviewed.
- The Company does not accept anonymous customers, shell entities without a verified UBO, or entities operating in high-risk jurisdictions without a clear legal basis.
- PEP exposure, sanctions risk, or unexplained funding are grounds for enhanced due diligence or rejection.
- CAP decisions are informed by the Customer Risk Assessment (CRA) scoring model and residual risk level.

7.2. Minimum Information Required for Acceptance

Before entering into a business relationship, the Company will obtain and verify minimum Information required for Acceptance as per Customer Due Diligence process.

A customers's acceptance status may be reassessed if:

- There are changes in the ownership structure or UBOs
- The customer moves into a high-risk jurisdiction
- There is a negative media event or sanctions hit
- The contract value significantly increases (e.g., >€50,000)
- Suspicious activity is identified or reported

7.3 Acceptance Categories Based on CRA Risk Levels

CRA Risk Rating	Acceptance Status	Conditions
Negligible to Low (1–5)	Accept	Standard CDD, annual review

Medium (6–10)	Accept with Conditions	EDD required, management approval, annual review and enhanced monitoring
High (11–19)	Conditional	Accept only with justification from compliance + senior management approval + quarterly monitoring
Extreme (20–25)	Reject	Not within Company’s risk appetite; onboarding refused

7.3 Contractual AML Obligations

All accepted customers must agree to:

- Implement and maintain their own AML/CFT controls
- Cooperate with information requests during monitoring or audits
- Notify the Company of changes to legal or ownership structure
- Accept contract clauses allowing for relationship termination in case of AML/CFT breaches

8. Customer Due Diligence (CDD)

8.1 Overview and Objectives

Customer Due Diligence (CDD) is the process of verifying and assessing the legitimacy and risk profile of a business relationship before and during engagement. It ensures compliance with AML/CFT obligations, supports the Company’s CRA methodology, and aligns with its Customer Acceptance Policy (CAP).

The objectives of CDD are to:

- Prevent fraud and financial crime by verifying entities and individuals;
- Ensure regulatory compliance with Curaçao, FATF, and international AML/CFT standards;
- Support CRA risk scoring, risk mitigation, and treatment decisions;
- Maintain transparency of customer ownership structures and business legitimacy.

8.2 Due Diligence Frequency

- CDD is performed at onboarding for all customers and updated at least annually.
- Additional reviews are triggered by:
 - Changes in ownership, jurisdiction, or company structure;
 - Adverse media or sanctions alerts;
 - Annual contract value increases above €50,000;
 - Identified risks during monitoring or CRA re-evaluation.

8.3 CDD Measures

The Company performs the following standard due diligence measures:

- Collect incorporation and registration documents;
- Verify Ultimate Beneficial Owners (UBOs), directors and key controllers;
- Check business license (if applicable by jurisdiction);
- Review the customers own AML policy, if applicable;
- Screen individuals and entities against:
 - Sanctions lists (UN, EU, Curaçao);
 - PEP status;
 - Adverse media search;
- Conduct ongoing due diligence when risk conditions change.

8.4 Know Your Business (KYB)

The Company verifies each business entity using the following documents:

- Certificate of Incorporation;
- Excerpt from commercial Register
- Business License (if applicable);
- Memorandum & Articles of Association;
- Shareholder Register;
- Ownership structure chart up to UBO level.

8.5 Know Your Customer (KYC)

KYC is applied to all UBOs, directors, authorised signatories, and corporate controllers. The following documentation is collected:

- Valid government-issued identity document (passport, IDs are not accepted);
- Proof of residential address (utility bill, bank statement);
- Screening for sanctions, PEP, and adverse media performed

For corporate directors, the following are required:

- Organigram signed by the director;
- Excerpt from corporate register;
- Shareholder register of the director entity;

If the contract value exceeds €50,000, the following are additionally required:

- Certificate of Good Standing;
- List of authorized signatories;
- Proof of Business Address (e.g., lease agreement, utility bill)

8.6 Know Your Supplier (KYS)

KYS is conducted for key service providers (e.g., game providers, technical vendors) to ensure legal operation and financial reliability.

Documentation includes:

- KYB equivalent (as above),
- Sanctions and media checks

8.7 Politically Exposed Person (PEP) Screening

All relevant individuals (UBOs, directors, signatories) are manually screened for PEP status using:

- Publicly available PEP registries (e.g., national PEP disclosures, listed politicians);
- Using resources such as:
 - [NameScan](#)
 - [DiliSense](#)
- Manual keyword-based Google searches

If a potential match is found:

- Additional review flagged and EDD triggered
- Senior management approval should be obtained before acceptance.

8.8 Manual Screening & Adverse Media Checks

Since automated tools are not in use, the Company performs manual searches using:

- Public domain search engines (e.g., Google);
- The following keywords combined with customer or individual names:
 - "sanction", "money laundering", "fraud", "scam", "criminal", "investigation", "regulatory fine", "FATF", "suspension", "gambling license revoked", "offshore".

Findings are documented and stored in the due diligence file. Any result suggesting material risk triggers EDD and escalation to the management.

8.9 Enhanced Due Diligence (EDD)

EDD is required in the following situations:

- Customer is based in a high-risk jurisdiction;
- Ownership has a complex structure;
- One or more individuals is a PEP;

- Adverse media or ongoing legal issues are detected;

EDD Measures:

- Declaration and verification of source of funds/wealth;
- Collection of additional corporate and financial documentation;
- Approval of senior management;
- Enhanced ongoing monitoring and file updates.

8.10 Recording Due Diligence Results

All CDD/EDD results are:

- Stored in structured electronic folders;
- Documented in a Due Diligence Summary Report;
- Include findings, links, screening outcomes, and CRA reference;
- Retained for five (5) years after end of relationship, in compliance with Curaçao law.

8.11 Ongoing Monitoring

The Company ensures ongoing monitoring by:

- Reviewing updates in license status, sanctions listings, and ownership changes,
- Conducting periodic review of high-risk customers

8.12 Reliance on Third Parties for CDD

The Company does not rely on third parties to perform CDD on B2C customers.

However, it ensures that its customers apply proper AML measures to their players and may request evidence of such compliance if necessary.

8.13 Record Keeping

All customer due diligence, risk assessments, contracts, and screening records are retained for at least five (5) years following the termination of the business relationship. The Company uses secure digital storage solutions with access limited to authorised compliance staff, in accordance with data protection laws.

9. Reporting of Unusual Transactions

While Viral Technology N.V. does not operate any player-facing business or handle individual wagers, it remains responsible for reporting any unusual transactions involving its customers. This includes:

- Payments received from or routed through high-risk jurisdictions without business justification;
- customers or beneficial owners appearing on sanctions or terrorism watchlists;
- Suspicious changes in customer behavior, ownership, or structure

All such cases will be escalated to Head of Compliance, and if deemed necessary, reported to the FIU Curaçao in compliance with reporting obligations under NORUT.

10. Anti-Money Laundering Compliance Program

Viral Technology N.V. maintains a risk-based AML/CFT compliance program designed to prevent the misuse of its services for money laundering, terrorist financing, or other illicit activity. The program includes:

- A documented AML policy and internal controls aligned with Curaçao laws and FATF standards;
- Risk-based customer due diligence and screening procedures customers;
- Regular risk reassessments of ongoing partnerships;
- Reporting obligations for suspicious or unusual corporate transactions;
- Internal escalation procedures and compliance oversight.

While the Company does not manage player funds or accounts, it retains responsibility for ensuring its customers' compliance integrity to avoid indirect exposure to financial crime risks.

11. Obligations towards B2C operators

11.1 As a reseller of casino games content Viral Technology requires the operator of the online casino ("operator", "the Website") where the games are offered to the public:

As a minimum:

- appoint one of its senior officers as the designated Money Laundering Reporting Officer (MLRO) whose responsibilities will include the duties required by the laws regulations and guidance notes
- take reasonable steps to establish the identity of any person for whom it is proposed to provide its service.

For this purpose, the process for the registration of Players under the General Terms and Conditions on the Website provides for the due diligence process that must be carried out before the opening of a User Account.

- keep at all times a secure online list of all registered Players.
- retain identification and transactional documentation as defined in the laws, regulations and guidance notes.

- ensure that this policy is developed and maintained in line with evolving statutory and regulatory obligation and advice from the relevant authorities.
- examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.
- cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity.

11.2 Moreover, operator shall:

- not accept to open anonymous Accounts or Accounts in fictitious names such that the true beneficial owner is not known.
- not register a Player who is under eighteen (18) years of age.
- only register a single account in the name of a particular person: multi-account practices are strictly prohibited.
- transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.
- not accept a wager unless a User Account has been established in the name of the Player and there are adequate funds in the Account to cover the amount of the wager.
- not accept a wager unless the funds necessary to cover the amount of the wager are provided in an approved way.
- if it becomes aware that a person has provided false information when providing due diligence documents, not register such person. Where that person has already been registered, the operator shall immediately cancel that person's registration as a Player with the company.

If a Player has been identified as attempting or participating in any criminal or unlawful activity, the Company will take the appropriate steps to immediately freeze the account of the Player.

If any material personal information of a Player changes, verification documents will be requested.

11.3 The Website will conduct ongoing monitoring and monitor account activity with special attention, and to the extent possible, the background and purpose of any more complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.

Parameters that signal possible money laundering or terrorist financing include, but are not limited to:

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent reason.
- Many small, incoming wire transfers or deposits made using checks and money orders.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent specific purpose.

When an employee of the Website detects any activity that may be suspicious, he or she will notify the MLRO, who will then determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.

To the extent the Website utilizes a third party to process and record payments to and from Player and accounts, the Website will use best efforts to ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in accordance with the applicable legislation. The AML Compliance Person shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

Records relating to the financial transactions shall be maintained in accordance with the data protection and retention requirements in the applicable jurisdiction of Curaçao.

11.4 The Website will take reasonable steps to establish the identity of any person for whom it is proposed to provide its service (hereinafter "Players"). For this purpose, the process for the registration of Players provided for under the General Terms and Conditions of the Website provides for the due diligence process that must be carried out before the opening of a user account. The Website will keep at all times a secure online list of all registered Players and information and documents will be retained in accordance with the applicable data protection obligations.

The Website will inform relevant Players that the Website may seek identification information to verify the identity of the Player.

Any employee of the operator who becomes aware of an uncertainty in relation to the accuracy and truthfulness of the Player information provided shall immediately notify the MLRO who will review the materials and determine whether further identification is required and or so that it may be determined whether a report is to be sent to the relevant authorities.

11.5 The AML Compliance Person will report to MLRO any suspicious transactions (including deposits and transfers) conducted or attempted by, at or through a Player account where the AML Compliance Person knows, suspects or has reason to suspect:

- The Player is included on any list of individuals assumed associated with terrorism or on a sanctions list;
- The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation;
- The transaction has no ordinary lawful purpose or is not the sort in which the Player would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- The transaction involves the use of the Website to facilitate criminal activity.

12. Training Programs

12.1 The Company will offer ongoing employee training under the leadership of the AML Compliance Person and senior management. The training will be updated as necessary to reflect any new developments in the law.

12.2 The training will include, at a minimum:

- how to identify red flags and signs of money laundering that arise during the course of the employees' duties;
- what to do once the risk is identified (including how, when and to whom to escalate unusual activity or other red flags for analysis);
- what employees' roles are in the Company's compliance efforts and how to perform them;
- the disciplinary consequences for non-compliance with legislation.

13. Compliance and Consequences of Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action including termination of employment or contract,
- Regulatory reporting and investigation,
- Suspension or termination of partnership.

14. Related Information

National Ordinance on the Identification of customers (NOIS)

<https://www.centralbank.cw/legislation-guidelines/integrity-financial-sector/anti-money-laundering>

National Ordinance on the Reporting of Unusual Transactions (NORUT)

<https://www.centralbank.cw/legislation-guidelines/integrity-financial-sector/anti-money-laundering>

CGB AML Regulations (2025) <https://www.gamingcontrolcuracao.org/regulation/aml>

FIU The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

<http://www.fiucuracao.cw/web/motweb/motweb.nsf/web/home?opendocument>

The Caribbean Financial Action Taskforce. (CFATF) [https://www.fatf-](https://www.fatf-gafi.org/en/countries/global-network/caribbean-financial-action-task-force--cfatf-.html)

[gafi.org/en/countries/global-network/caribbean-financial-action-task-force--cfatf-.html](https://www.fatf-gafi.org/en/countries/global-network/caribbean-financial-action-task-force--cfatf-.html)

International related information

The Financial Action Task Force. (FATF) <https://www.fatf-gafi.org/en/countries/fatf.html>

15. Contact Information

For any questions regarding this policy:

eMoore N.V.

Legal and Compliance Department

Groot Kwartierweg 10, Livestrong Building Willemstad, Curaçao

Telephone: [+599 9 7471401](tel:+59997471401)

Email: legalcompliance@the-emgroup.com

Email: compliance@21viral.com