

Anti-Money Laundering/ Combating Financing of Terrorism Policy

- CONFIDENTIAL -

This Document is intended only for the following users:

<u>User Types</u>
General Users (All Employees)

Version Control:

<u>Document Version</u>	<u>Responsible Office:</u>	<u>Approving Official</u>	<u>Document Purpose</u>	<u>Release Date</u>	<u>Signature for Approval</u>
1.0	Dmitrii Shchikovskii – Compliance Officer	Ersilia Vivian Victoria, (SMES) Solution for Management and Employment Support N.V.– Director	Initial Release	May 27, 2025	<i>Signed in original. Signature retained in compliance files.</i>
1.1	Dmitrii Shchikovskii – Compliance Officer	Ersilia Vivian Victoria, (SMES) Solution for Management and Employment Support N.V.– Director	Regulatory Update: Amendments to comply with GCB January 2025 Regulations, BO/Syndicate Funding controls, and Ministerial Decree 2015 Indicators	December 11, 2025	 (SMES) Solutions for Management and Employment Support N.V.

TABLE OF CONTENTS

1. POLICY STATEMENT.....	5
2. PURPOSE.....	5
3. AUDIENCE.....	5
4. DEFINITIONS.....	6
5. ML/TF/FP RISK BACKGROUND	9
6. POLICY IMPLEMENTATION	13
6.1. Introduction.....	13
6.2. Business Risk Assessment (BRA)	13
6.2.1. Objective and Scope.....	13
6.2.2. Methodology of BRA	15
6.2.3. Risk Scoring Methodology Explained.....	15
6.2.4. Controls and Risk Mitigation Measures	18
6.2.5. Documentation and Review	18
6.2.6. Scoring Methodology and Integration with Customer Risk Score	18
6.2.7. Internal Controls – Implementation of the Risk-Based Approach	19
6.2.8. First Line of Defence – KYC and Onboarding Staff	19
6.2.9. Dynamic Risk Management.....	20
6.3. Customer Acceptance Policy.....	21
6.3.1. Failure or refusal to submit information.....	21
6.3.2. General Principles of the CAP are the following	22
6.3.3. Criteria for Accepting New Customers (based on their respective risk).....	23
6.3.4. Low-Risk Customers	23
6.3.5. Medium Risk Customers.....	23
6.3.6. High Risk Customers.....	23
6.3.7. Player Registration	24
6.3.8. Email Verification.....	24
6.4. Customer Risk Assessment (CRA).....	24

6.5.	Customer Due Diligence	26
6.5.1.	Simplified Due Diligence	26
6.5.2.	Customer Due Diligence.....	27
6.5.3.	Enhanced Due Diligence.....	27
6.5.3.1	Beneficial Ownership and Third-Party/Syndicate Funding Controls.....	28
6.5.4.	Customer identification and verification guidelines.....	29
6.5.5.	Sanction List Screening.....	31
6.5.6.	Player Verification Procedure	32
6.5.7.	Applied Due Diligence Measures and Account Controls Breakdown	34
6.6.	Ongoing monitoring.....	41
6.6.1.	The customer risk profile contains the following fields.....	42
6.6.2.	Format of Records	45
6.6.3.	Certification and language of documents	45
6.6.4.	Procedures	46
6.6.5.	Timeframes.....	47
6.6.6.	Payout Management Procedure	47
6.6.7.	Dormant Accounts	49
6.7.	Reliance on Third Parties to perform Customer Due Diligence	49
6.8.	Unusual Transaction Reporting	49
6.8.1.	Internal reporting and escalation procedure	51
6.8.2.	Knowledge	52
6.8.3.	Compliance Officer's report to the FIU	53
6.8.4.	Submission of information to the FIU.....	53
6.9.	AML Compliance Program	54
6.10.	Record keeping and monitoring	55
6.11.	Independent audit	56
6.12.	Examination by the Curaçao Gaming Authority (CGA)	57
7.	AML GOVERNANCE & RESPONSIBILITIES	57

Carletta N.V. – Anti-Money Laundering Compliance Policy

8. EMPLOYEE TRAINING PROGRAM.....	61
8.1. Employees' obligations	61
8.2. Employees' Education and Training.....	61
8.3. Compliance Officer Education and Training Program	62
9. CONSEQUENCE OF NON-COMPLIANCE (NOIS and NORUT)	62
9.1. Sanctions for Non-Compliance	63
9.2. Personal Liability of Responsible Officers	63
10. AGENTS/INTERMEDIARIES	63
11. RELATED INFORMATION	63
12. CONTACT INFORMATION.....	64
ANNEX A - Internal Control Structure: Three Lines of Defense.....	65
ANNEX B - Trigger-Based Risk Scoring Table	67
ANNEX C - Jurisdiction Risk Classification and Prohibited Countries List	70
ANNEX D - Standardized template of the Internal Suspicion Report (ISR).....	73
ANNEX E - Annual AML/CFT Training Plan	75
ANNEX F - Examples of unusual transactions/activities related to money laundering and terrorist financing	77
ANNEX G - Employee screening program.....	80
ANNEX H - Responsibilities of the Compliance Officer as required by the CGA.....	81
ANNEX I – Ongoing employee training program	82

1. POLICY STATEMENT

This Anti-Money Laundering/ Combating Financing of Terrorism Policy (“the Policy”) outlines the practical framework adopted by Carletta N.V. to ensure full compliance with applicable AML/CFT obligations under Curaçao law. The Policy reflects the Company’s commitment to detecting, preventing, and reporting any attempt to use its services for money laundering, terrorist financing, or other financial crimes.

This Policy is designed and maintained in accordance with the Curaçao Gaming Control Board (GCB) AML/CFT Regulations (January 2025), which constitute the governing regulatory standard for AML/CFT compliance. Carletta N.V. confirms that all AML/CFT controls, procedures, due diligence measures, and reporting obligations contained in this Policy comply with the January 2025 GCB Regulations.

The Policy defines the operational procedures and control mechanisms implemented across the Company’s business activities, including customer onboarding, identification and verification, customer risk assessment, ongoing monitoring, unusual transaction detection, staff training, and regulatory reporting.

This Policy applies to all departments, employees, managers, compliance personnel, onboarding specialists, and third-party service providers who are involved in any function that affects the Company’s AML/CFT risk exposure. The Policy is designed and maintained in line with the Curaçao AML/CFT Regulations (2024), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and applicable FATF recommendations.

2. PURPOSE

The purpose of this Policy is to establish a risk-based, structured approach for identifying and preventing the misuse of Carletta N.V.’s operations for money laundering or terrorist financing. The Policy ensures that effective procedures, controls, and internal responsibilities are in place to fulfill legal and regulatory obligations in Curaçao and to protect the Company from reputational, financial, and regulatory risk.

3. AUDIENCE

This Policy applies to:

- All employees of Carletta N.V., including management and board members;
- Any person responsible for customer-facing functions, transaction processing, or risk-related decisions;
- External KYC and onboarding providers contracted by the Company;

Carletta N.V. – Anti-Money Laundering Compliance Policy

- Any current or future third-party providers or subcontractors engaged by the Company to perform compliance-related functions, including KYC and onboarding services.

All such individuals are required to read, understand, and comply with the measures outlined in this Policy.

4. DEFINITIONS

For this Anti-Money Laundering Compliance Policy, unless the context shall prescribe otherwise:

“Anti-Money Laundering/ Combating Financing of Terrorism Policy” (hereinafter also referred to as **“Policy”**) – sets out the Company’s commitment and procedures for managing anti-money laundering and counter-terrorist financing risks. It encompasses the full AML Compliance Program, including the risk-based assessment of business and customers (BRA and CRA), due diligence measures (CDD/EDD), transaction monitoring, internal controls, reporting mechanisms, employee training, staff screening, and independent audits, as required by Curaçao AML/CFT Regulations.

“Anti-Money Laundering Compliance Program”, “Program” means Company’s Anti-Money Laundering and Counter Financing of Terrorism Policies and Procedures.

“Beneficial Owner” means the natural person or natural persons, who ultimately own or control the Customer and/or the natural person on whose behalf a transaction or activity is being conducted.

“Business Relationship” means a business, professional, or commercial relationship connected with the professional services offered by the Company, and which was expected, at the time when the contract was established, to have an element of duration.

“Business Risk Assessment (BRA)” – a structured process aimed to identify, evaluate, and manage the risks the Company faces in the context of money laundering (ML), financing of terrorism (FT) and proliferation of weapons of mass destruction (FP).

“Carletta”, “Company” means Carletta N.V., a limited liability company that is duly incorporated under the Laws of Curaçao and its related companies and entities.

“CDD” – Customer Due Diligence.

“CFATF” – The Caribbean Financial Action Taskforce. An organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement

common countermeasures to address money laundering.

“Compliance Officer” – A senior officer at the management level and independent from the game's operations, responsible for detecting and deterring money laundering and terrorist financing.

“Customer” (hereinafter also referred to as **“Player”**) means any natural person who interacts with the Company's services, including real-money gaming, deposits, withdrawals, or other transactions.

“EDD” – Enhanced Due Diligence, includes additional verification procedures applied to high-risk customers or situations, including PEPs, unusual transactions, or high-value behavior.

“FATF” – the Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

“FATF Recommendations” – a framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction.

“Financial Transactions” – in casinos these include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers, and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens.

“FIU” – The Financial Intelligence Unit Curaçao, as it is referred to in Art. 2 of the NORUT.

“Kingdom Sanctions Act” - The National Ordinance also known as the “Rijkssanctiewet”, published under N.G. 2016 no. 54.

“KYC” – Know Your Customer.

“Law” means any Laws and Acts legally enacted from time to time in Curaçao, or which are applicable and enforceable in Curaçao.

“Money Laundering and Terrorist Financing” or **“ML/TF/FP”** means the money laundering offenses and terrorist financing offenses defined in the Law.

“National Risk Assessment” – The country-wide assessment coordinated by authorities to

Carletta N.V. – Anti-Money Laundering Compliance Policy

understand the ML/TF/FP risks in Curaçao.

“NOIS” – National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92, a.a.).

“NORUT” – National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99, a.a.).

“Occasional Transaction” means any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of gaming or related services.

“Ongoing Monitoring” – The continuous review of customer behavior, transactions, and risk level to ensure they remain consistent with the Customer’s known profile.

“Politically Exposed Persons (PEPs)” – foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, and the direct family members or close associates of such persons. Examples are Heads of State or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, and important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refer to members of senior management, i.e. directors, deputy directors, and members of the board or equivalent functions.

“Regulations” – Curaçao Gaming Authority’s Regulations for the Combating of Money Laundering, the Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction as may change from time to time.

“RBA” - Risk Based Approach, means a core AML principle requiring the Company to apply measures proportionate to the level of risk posed by a Customer or transaction.

“Sanctions National Ordinance” – the National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 2014 no. 55.

“Sanctions Screening” – the process of checking Customers against relevant national and international sanctions lists (UN, EU, OFAC, etc.).

“Source of Funds” – refers to how the funds for a particular transaction were obtained by the

Carletta N.V. – Anti-Money Laundering Compliance Policy

Player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, and compensation from legal rulings.

“Source of Wealth” – source of wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, and business ownership interests.

“SDD” – Simplified Due Diligence, includes reduced level of due diligence applied in low-risk situations, as permitted under a risk-based approach.

“Tipping off” - The act of informing a Customer or third party, either directly or indirectly, that they are the subject of an unusual transaction or suspicious transaction report (STR), investigation, or enhanced scrutiny by a financial institution, gaming operator, or regulatory authority.

“Ultimate beneficial ownership (UBO)” – Refers to the natural person(s) who ultimately own(s) or control(s) a Customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

“Unusual transaction” – Any transaction that deviates from a Customer's expected activity or appears unusual based on objective or subjective indicators and is considered as such under Article 10 of the NORUT.

“UTR” – Unusual Transaction Report.

“XCG. 4,000 threshold” means the threshold when all CDD measures must have been conducted at the time it's reached.

5. ML/TF/FP RISK BACKGROUND

This document constitutes Carletta N.V.'s AML/CFT Compliance Program in accordance with CGA requirements and shall be referred to hereafter as “the Policy”. The document shall indicate and define the Company's policies and procedures intended to prevent its products and/or services from being used for ML/TF/FP purposes. This document shall set the standard to be followed by the Company, its officers, and employees, the measures and controls in place, and the internal practices to follow. The Policy shall be reviewed yearly to determine if any updates and/or amendments are required. The frequency of such updates can be higher should there be any regulatory change or change in the policies and procedures to be applied due to any change in the risks faced by the Company or due to any changes in the assessment of certain risk factors arising out of publications made by the FIU, FATF, and National Risk-Assessments. It shall be the

Carletta N.V. – Anti-Money Laundering Compliance Policy

Compliance Officer's responsibility to ensure that this document is reviewed and updated if and when required. Any updates and/or changes made to this document shall be presented to the board of directors, who shall review and approve such changes.

The Company strives to ensure that all possible efforts are undertaken to prevent money laundering or the funding of terrorism and proliferation and actively acts to curtail such illicit activity. The Company complies with the Kingdom Sanctions Act, NOIS, NORUT, the Curaçao Gaming Control Board (GCB) AML/CFT Regulations (January 2025), Sanction National Ordinance, EU Directives on the Prevention of Money Laundering and Funding of Terrorism, and any other applicable laws and regulations.

Money laundering is an offense by which money derived from criminal activity is passed through a series of processes to disguise the ownership and management of such revenue, which therefore cannot be traced back to the underlying crime. The process of money laundering makes such funds appear to have been generated from legitimate sources of business.

The stages of money laundering are as follows:

- I. Placement
- II. Layering
- III. Integration

Placement

Placement is the stage where the money is introduced into the financial system, the funds at this stage are still illegitimate, and the launderer will try to incorporate and place the funds derived from **illicit** activity into the system to start the process of money laundering. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits. At this stage, it is essential to understand where the money originates from, as the person who intends to commit such an act will need to obfuscate any link between the funds and criminal activity without attracting any attention, for example through structuring or smurfing. "Structuring" refers to the practice of breaking down a large financial transaction into smaller, separate transactions to avoid triggering reporting thresholds required by regulators. "Smurfing" is a form of structuring that involves illegally obtained funds and the use of low-level financial criminals, known as 'smurfs'.

Layering

At this stage, the funds have been deposited in the financial institution. It is at this point that layering is used through complex structures directed to lose all trace of the money and remove any trace of its origination from the proceeds of a crime. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities. This process is intended to ensure that the funds are as far removed as possible from the proceeds of a crime.

It is important to prevent such an event by transaction by ensuring staff are equipped to ask the right questions whilst avoiding alerting the Customer of any suspicion. Tipping off a money launderer can have severe penalties, so all staff are regularly trained in how to detect at which point a transaction is out of their comfort zone and how to interact in a way that would not alert the individual making the transaction of any suspicion.

Integration

At this stage, the money derived from criminal activity has been made legitimate and placed once again into the financial system as legitimate funds. At this stage, the launderer has been successful in laundering the funds.

Terrorist Financing

When dealing with the issue of terrorist financing, an important aspect is that the money does not necessarily have to be derived from criminal activity. The funds may be legitimate. It is not a case of disguising the source of the funds but simply the intentional transfer of funds from A to B with the intention of the receiver using those funds to support terrorist activity.

The intent and the scope of such acts are different and differ from case to case, but the process used for the funding of terrorism can be fairly like those methods used for money laundering.

Proliferation financing

In essence, proliferation financing supports the spread of weapons of mass destruction (WMDs) by enabling the financial transactions and logistics behind their development and distribution, posing a serious global security risk. It is the act of providing funds or financial services for the manufacture, acquisition, development, or transport of WMDs, such as nuclear, chemical, or biological weapons, and their delivery systems.

Key aspects of proliferation financing are that the funds may come from legitimate sources (e.g., companies, state actors), the end-use of the funds is illicit, violating international laws and

Carletta N.V. – Anti-Money Laundering Compliance Policy

sanctions, and it often involves complex trade and financial structures, including front companies, dual-use goods, and evasion of sanctions.

Comparison between ML, TF, and PF

Aspect	Money Laundering (ML)	Terrorist Financing (TF)	Proliferation Financing (PF/WMD)
Source of Funds	Typically from criminal or illicit activity (e.g., drugs, fraud).	Can be from legal or illegal sources (e.g., salaries, donations, or crime).	Often from legitimate sources, including companies and states.
Purpose	To disguise the illicit origin of funds and integrate them into the legal economy.	To fund terrorist groups or acts, regardless of the legality of the funds' origin.	To fund the development, production, acquisition, or transport of WMDs and related materials.
Criminal Element	The source of the funds is criminal.	The use or destination of the funds is criminal.	The purpose and end-use of the funds is criminal under international law.
Complexity of Methods	Often involves multiple stages: placement → layering → integration.	May use simple or informal transfer channels; emphasis on concealment of intent.	May involve complex trade finance structures, front companies, or sanctions evasion tactics.
Red Flags	Use of shell companies, high-value transactions, inconsistent business activity.	Small or structured transactions, links to NPOs or sanctioned regions.	Involvement in dual-use goods, unusual trade routes, links to high-risk jurisdictions or sanctioned entities.
Key Controls	CDD, transaction monitoring, UTRs, EDD, recordkeeping.	CDD, ongoing monitoring, sanctions screening, UTRs, NPO due diligence.	Sanctions screening, trade finance scrutiny, EDD, screening against WMD proliferation lists (e.g., UN, OFAC).

6. POLICY IMPLEMENTATION

6.1. Introduction

The Company is aware of the stages of ML/TF/FP and ensures to take all preventative measures to combat, prevent, and detect ML/TF/FP. Prevention is ensured by carrying out the following measures:

- Implement policies and procedures throughout the group of companies.
- Communicate such policies and procedures to staff.
- Adopt a risk-based approach.
- Internal Controls.
- Customer due diligence procedures.
- Record keeping and Monitoring.
- Unusual activity reporting.
- Training.

The Company applies a combination of manual and automated customer due diligence and verification processes, conducted by the Compliance department and supported by technical tools, in line with the nature and scale of its operations and knowledge of its Player database. In any case where a transaction is complex, unusually large, or exhibits an atypical pattern inconsistent with the Customer's known profile, such transaction is flagged – either by the system or manually – as unusual, and an internal investigation is initiated without delay.

The AML Regulations impose prevention and enforcement for subject persons. Therefore, Carletta N.V. applies the risk-based approach to prevent and detect fraud.

The risk-based approach is operationalized through a formal **Business Risk Assessment (BRA)**, which evaluates the Company's exposure to ML/TF/FP risk across key dimensions such as products, delivery channels, geography, customer types, and transaction behavior. The BRA serves as the foundation for Customer Acceptance Policy (CAP), risk scoring, and due diligence procedures.

6.2. Business Risk Assessment (BRA)

6.2.1. Objective and Scope

Carletta N.V. conducts an annual Business Risk Assessment (BRA) to identify, understand, and mitigate the money laundering, terrorist financing, and proliferation financing (ML/TF/FP) risks it is exposed to, as required under Curaçao AML/CFT Regulations and in line with international standards such as the FATF recommendations.

Carletta N.V. – Anti-Money Laundering Compliance Policy

The purpose of the Business Risk Assessment (BRA) is to define the Company's exposure to ML/TF/FP risks across its operations and support the design of internal policies, procedures, and control mechanisms. Although the BRA may apply a different internal risk scale (e.g., Likelihood × Impact) for strategic or organizational analysis, its findings directly inform the structure of the Customer Risk Assessment (CRA), including the identification of risk categories, the selection of relevant risk factors, and the assignment of scoring weights.

In this way, the Company translates BRA conclusions into specific operational risk triggers used in the CRA scoring model (ranging from 1 to 3 points per trigger). This ensures a consistent and traceable link between enterprise-level risk awareness and individual customer risk classification and decision-making.

The BRA covers:

- customer profiles;
- jurisdictions served;
- products and services offered;
- delivery channels;
- transaction types and patterns;
- technological risks.

The BRA ensures that internal AML/CFT policies, controls, and procedures are risk-proportionate and adapted to Carletta N.V.'s business model, customer base, and regulatory obligations.

The following steps are followed by Carletta N.V. to operationalize the risk-based approach derived from the Business Risk Assessment:

Identification – The Company identifies internal and external ML/TF/FP risks that may impact its business. This includes risks related to customer profiles, target jurisdictions, products, and the delivery channels used. Particular attention is given to risks originating from jurisdictions known to be non-compliant with AML standards or associated with heightened financial crime risks. The BRA is reviewed annually or more frequently as needed to account for new or emerging threats.

Assessment – As an online gaming operator, the Company understands and is aware that there is susceptibility to a certain level of high risk. Furthermore, management must stimulate awareness to detect the lack of implementation of stringent measures to detect fraudulent activity; the sites may become an easy target to launder money, and this is a clear example of inherent risk. In carrying out the risk assessment required, the Company must:

Monitoring and Follow-up – The Company scrutinizes the risk assessments carried out to recognize gaps in procedures and areas of improvement in procedures to reduce inefficiencies. It is important to note that inefficiencies may be present in both procedures and a lack of technical expertise adopted by staff.

Supervise and train – The Company ensures that all relevant staff receive training based on the identified risks and changes in the regulatory environment. Risk management processes are reviewed regularly by the Compliance Officer and adjusted as needed to reflect current obligations.

6.2.2. Methodology of BRA

The BRA is carried out using a structured risk-based methodology:

- Risk categories: Customer risk, geographic risk, product/service risk, delivery channel risk, transaction behavior risk;
- Scoring system: Each risk factor is scored based on likelihood (1–4) and impact (1–4), resulting in an inherent risk score (1–16);
- Review frequency: Annually, or sooner if triggered by regulatory, operational, or market changes.

The Compliance Officer leads the BRA and ensures Board-level review and approval.

6.2.3. Risk Scoring Methodology Explained

Carletta N.V. uses a dual-factor risk scoring methodology that considers the **likelihood** of a risk event occurring and the **impact** it may have. Each risk is evaluated using the following principles:

- **Likelihood** is scored from 1 to 4, based on historical occurrence, process complexity, and probability of the event materializing, 1 being least likely and 4 being most likely.
- **Impact** is scored from 1 to 4 and includes potential financial loss, reputational damage, operational disruption, and legal/regulatory exposure, 1 being least impactful and 4 being most impactful.

The Inherent Risk Score, the risk score in the absence of internal controls, is calculated as:

Likelihood × Impact → resulting in a score from 1 (low) to 16 (high).

Carletta N.V. – Anti-Money Laundering Compliance Policy

Each inherent risk is assessed using a Likelihood × Impact model (1–4), resulting in a total score between 1 and 16. Risk levels are categorized as Low, Medium, or High as depicted in below table and matrix.

Inherent risk scores	Risk category
1, 2, 3, 4	Low
6, 8, 9	Medium
12, 16	High

Inherent Risk Score		Likelihood			
		1	2	3	4
Impact	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Politically Exposed Persons (PEPs) are treated as a separate category, requiring enhanced due diligence regardless of score.

The table below summarizes the Company's internal prioritization of key ML/TF/FP risk categories based on the Business Risk Assessment (BRA).

Carletta N.V. – Anti-Money Laundering Compliance Policy

Risk Category	Risk Description	Likelihood	Impact	Total Score (L×I)	Risk Level	Primary Controls
Delivery Channel Risk	Use of unregulated or anonymous PSPs (e.g., crypto, vouchers)	4	4	16	High	Restricted acceptance, EDD, transaction limits, CO approval
Product/Service Risk	High-turnover, low-engagement gaming (e.g., crash, auto-play)	3	4	12	High	Monitoring by game type, bonus limitation, SoF checks
Geographic Risk	Customers from FATF high-risk or CPI-flagged jurisdictions	4	3	12	High	Geo-IP filtering, enhanced verification, SoW/SoF required
Customer Risk	High-risk individuals, frequent ID discrepancies, false profile	3	4	12	High	EDD, account limits, manual verification, document authentication
Transaction Behavior	Structuring, churning, suspicious deposit/withdrawal patterns	3	3	9	Medium	Pattern detection, automated flags, alert routing to Compliance
Technology Risk	VPN/proxy access, device manipulation, multiple accounts	3	2	6	Medium	Multi-account detection
PEP (Separate Category)	Politically Exposed Persons and their family members and close associates	N/A	N/A	N/A	PEP	Full EDD, SoW/SoF, senior management approval

NOTE: The risk scores of all relevant individual risks as recognized in the Business Risk Assessment (BRA) are applied in a weighted manner to each individual Customer, to determine whether a Customer is to be treated as low, medium or high risk. These risk designations are then

Carletta N.V. – Anti-Money Laundering Compliance Policy

scored as 1, 2, or 3, respectively, which serve as risk triggers in the Customer Risk Assessment (CRA). Each trigger contributes to Player risk reassessment and may initiate EDD and/or UTR filing. A detailed, but not exhaustive, list of behavioral and transactional triggers used in the Company's AML risk scoring model is provided in **Annex B – Trigger-Based Risk Scoring Table**.

6.2.4. Controls and Risk Mitigation Measures

Carletta N.V. applies proportionate AML/CFT controls tailored to customer risk levels. These include both automated and manual mechanisms to detect, review, and respond to identified risks.

Specific due diligence controls applied to customer accounts – based on their risk score – are described in detail in Section **6.5.7. “Applied Due Diligence Measures and Account Controls Breakdown”** of the Policy.

Control mechanisms include, but are not limited to:

- Risk-based CDD and EDD
- Sanctions and PEP screening
- Transaction monitoring and manual escalation
- Identity and behavior verification
- Multi-level review and approval process
- Ongoing monitoring based on risk level

6.2.5. Documentation and Review

An executive summary of the BRA is provided to the Board. Any material change in business model, client base, or regulatory framework triggers an immediate reassessment.

The BRA and CRA shall be reviewed and formally approved by the Board of Directors at least annually. Carletta N.V. shall retain full BRA/CRA documentation and make these documents available to the Gaming Control Board (GCB) upon request without delay.

6.2.6. Scoring Methodology and Integration with Customer Risk Score

Each risk factor listed in this Policy contributes to the overall Customer Risk Score on a weighted basis. The Company uses a numerical scoring model in which inherent risks are assigned a value between 1 and 3 points depending on severity. Scores are aggregated across five core categories: Customer, Geographic, Product, Delivery Channel, and Behavior. The cumulative score determines the Customer's risk classification and applicable level of due diligence.

The resulting total Risk Score determines the **Customer's risk classification**:

- **Low Risk:** Score 1 → Basic CDD
- **Medium Risk:** Score 2 → CDD + increased monitoring (Level 2 controls)
- **High Risk:** Score 3 → Full EDD required + Level 3 controls
- **PEPs:** Regardless of score → Classified separately and subject to mandatory full EDD, including SoW and SoF (Level 4 controls).

The system is designed to dynamically reassess the Risk Score based on Player behavior and trigger detection, including but not limited to: login anomalies, payment inconsistencies, transaction patterns, or document mismatch. These inputs are monitored both manually and through automated detection.

This scoring methodology ensures a consistent, measurable and proportionate application of due diligence based on the assessed ML/TF/FP risk.

6.2.7. Internal Controls – Implementation of the Risk-Based Approach

Following the identification of inherent risk, management is required to implement appropriate internal controls to mitigate such risks. These controls are structured and executed through the Company's Three Lines of Defense model, which clearly allocates responsibilities across operational teams, compliance oversight, and audit assurance. A detailed description of the internal control structure is provided in **Annex A – Three Lines of Defense**. The applied Account Controls Breakdown may be found in Section 6.5.7. "**Applied Due Diligence Measures and Account Controls Breakdown**" of the Policy.

6.2.8. First Line of Defence – KYC and Onboarding Staff

A third-party KYC service provider (hereinafter, the "KYC Provider") — KYCAID LIMITED — is engaged by the Company to carry out specific onboarding, identification, and customer due diligence tasks. This provider forms part of the **first line of defense** in the Company's AML/CFT framework.

Their key responsibilities include:

- Performing Customer Due Diligence (CDD).
- Monitoring for incomplete, inconsistent, or high-risk data.
- Ensuring proper documentation is gathered to determine whether a Customer fits the Company's risk appetite.

Carletta N.V. – Anti-Money Laundering Compliance Policy

The first line of defense must have adequate knowledge of the CAP and be able to apply it effectively in line with the Company's risk-based approach. All processes executed by the KYC Provider are subject to ongoing oversight by the Compliance Officer. Final responsibility for due diligence decisions and AML compliance remains with the Company.

In addition to the KYC Provider, other teams within the first line of defense are responsible for conducting initial behavioral assessments of Customers. These teams monitor unusual patterns, inconsistencies, or potentially suspicious activity, and escalate relevant findings to the Compliance Officer. Their role includes supporting the risk-based approach by contributing to customer risk classification prior to or in parallel with due diligence reviews.

6.2.9. Dynamic Risk Management

The Company is committed to maintaining a robust and proactive AML/CFT compliance structure in accordance with the expectations of the Curaçao Gaming Authority (CGA). In line with the CGA's guidance, the Company's risk management measures include the following components:

- Implementation of policies and procedures throughout the group of companies.
- Communication of such policies and procedures to all relevant staff.
- Adoption of a risk-based approach across all AML/CFT functions.
- Development and enforcement of internal controls.
- Application of customer due diligence procedures.
- Record keeping and ongoing transaction monitoring.
- Timely identification and reporting of unusual activity.
- An employee screening program
- Ongoing employee training programs tailored to AML/CFT obligations.
- An independent audit function to test the AML program.

The Company further embeds risk management through the application of documented Customer Acceptance Policies (CAP), structured Customer Risk Assessment (CRA) procedures, and a defined internal control framework. These are supported by comprehensive compliance management practices and formal communication of all related policies, procedures, and controls.

The Company ensures that all measures are clearly documented, approved by the Board of Directors, and understood by staff. Ongoing employee training and employee screening policies and procedures support the integrity of implementation across all levels of the business.

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities and requests change as well as the

services they require to be provided.

In this respect, the Compliance Officer must undertake regular reviews of the characteristics of existing Customers, new Customers, services, and the measures, procedures, and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented as per the requirements of the Policy, as applicable, and form part of the Annual Money Laundering Report.

It is also important for the Compliance Officer to monitor and ensure that the proper procedures are being implemented, and the risk-based approach principle is truly being followed in all areas of the Company. By doing so, one will also be ensuring that although certain products or Customers may be of a higher risk, the Company may continue providing these services and assisting these Customers due to the risk being mitigated through the proper policies being implemented.

6.3. Customer Acceptance Policy

The Customer Acceptance Policy (hereinafter the “CAP”), follows the principles and guidelines described in this document, defines the criteria for accepting new Customers, and defines the Customer categorization criteria that shall be followed by the Company and especially by the employees who have direct involvement in the obtainment of information and data relating to the Customer as well as employees who will be tasked with evaluating such Customer information to make recommendations as to whether such Customer falls within the Company’s risk appetite in so far as the products or services being provided are concerned.

The Compliance Officer shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, by the provisions of this policy, or at any other such interval as may be determined from time to time based on any changes in the Company’s inherent risk.

6.3.1. Failure or refusal to submit information

Customers who fail or refuse to submit and provide the Company with the requisite data, information, and/or documentation for their identification and verification and the creation of their profile, after they have reached the relevant thresholds (hereinafter referred to as the “thresholds”) i.e. XCG 4,000 threshold deposits, first withdrawal or due to an increase in the Customer risk profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Customer is involved in money laundering or terrorist financing activities, although this cannot be taken as an absolute and more investigation may be required before coming to such conclusion. In such an event, the Company shall suspend the Customer’s account or the

Carletta N.V. – Anti-Money Laundering Compliance Policy

execution of the transaction while at the same time, the Compliance Officer must also consider whether it is justified under the circumstances at hand to submit a report to the FIU.

If, during the Business Relationship or pending the execution of a transaction, the Customer fails or refuses to submit, within a reasonable timeframe (30 days from the date upon which the relevant threshold or circumstances have become effective), the required verification data and information by this document, the Company terminates the Business Relationship, provided that doing so does not result in a breach of the anti-tipping off obligation. The relevant report of the transaction should be submitted to the FIU.

6.3.2. General Principles of the CAP are the following

- (b) the Company shall classify Customers and/or products into various risk categories and, based on the risk perception attached to such classifications will determine the amount and quality of information and documentation which will be required for a Customer to be accepted or rejected. Such information and data must not be below the minimum requirements as set in the FIU and CGA implementing procedures and the AML Laws and EU Directives in force at the time
- (c) Customers may only sign up and be allowed to make use of the Company's products and services if they provide the following information: (a) name and surname; (b) permanent residential address; (c) date of birth; (d) place of birth; (e) nationality; and (f) identity reference number where applicable. However, in low-risk scenarios, Carletta N.V. may limit identification to the three personal details set out in (a) to (c) above.
- (d) all documents and data described in this policy must be collected before the Customer is permitted to continue using the services once the thresholds have been reached (such as identity documentation and proof of residence); otherwise, access to the services will be temporarily suspended until the required information is provided. no services shall be provided to anonymous Customers or Customers who are known to be operating under fictitious names(s)
- (e) no services shall be provided to high-risk Customers unless the prospective Customer is approved by:
 - one of the Company's Directors and/or Senior Managers or
 - the Compliance Officer.
- (f) the Company accepts Customers strictly on an individual, natural-person basis and does not onboard corporate or legal-entity Customers.
- (g) the Company prohibits the funding of Player accounts through corporate bank accounts, business payment instruments, or pooled/syndicated financial arrangements. Any indication that a Player account is funded, controlled, or beneficially owned – directly or indirectly – by a third party or a corporate structure shall trigger Enhanced Due Diligence (EDD), account restrictions, or rejection in accordance with this Policy.

6.3.3. Criteria for Accepting New Customers (based on their respective risk)

This Section describes the criteria for accepting new Customers based on their risk categorization. Following a risk-based approach, one must on a case-by-case basis determine what level of due diligence should be applied on identification, business relationship, and transaction level, provided that these do not fall below the minimum as set out by the various applicable laws and regulations in place at the time. Whether the level of risk is above or below the threshold the Company is willing to undertake, one needs to be able to provide evidence to regulatory bodies that the appropriate steps have been taken to mitigate risk. There are three commonly recognized categories of due diligence.

6.3.4. Low-Risk Customers

The Company shall accept Customers who are categorized as low-risk Customers if the general principles discussed in the sections below are applied.

Moreover, the Company shall follow the *Simplified Customer Identification and Due Diligence Procedures* for low-risk Customers, as defined in this Policy, and apply Level 1 controls.

6.3.5. Medium Risk Customers

The Company shall accept Customers who are categorized as medium-risk Customers by the general principles as defined in this Policy, and who shall be subject to standard customer due diligence (CDD) and Level 2 controls.

6.3.6. High Risk Customers

The Company shall accept Customers who are categorized as high-risk Customers by the general principles under Section **6.5.7. “Applied Due Diligence Measures and Account Controls Breakdown”** of the Policy.

Moreover, the Company shall apply the *Enhanced Due Diligence* measures for high-risk Customers, in accordance with the Policy and the specific identification and verification procedures applicable to such Customers (Level 3 controls).

The Company will also classify the risk further to ensure that adequate attention is given to the Customers under their respective risk profiles. For this reason, the 3 main risk categories are classified as Low, Medium, and High or PEP, based on the risk score assigned in the Customer Risk Assessment. Such an approach ensures that the measures taken to ensure the detection of any

Carletta N.V. – Anti-Money Laundering Compliance Policy

ML/TF/FP are more targeted to the respective risk levels.

6.3.7. Player Registration

To open an account with Carletta N.V. via the web portal, a user must first complete the registration process and deposit some funds with which he/she can then start playing. The Company applies a risk-based approach and ensures that identification requirements align with the level of risk posed by the Player.

In accordance with the requirements of the Curaçao Gaming Authority, the Company collects the following mandatory information from new Players:

- the first and last name,
- permanent residential address,
- date of birth,
- place of birth,
- nationality,
- identity number.

In addition, the Company may also collect e-mail address, phone number, and account currency.

In low-risk scenarios, the Company may limit the required data to full name, permanent address, and date of birth. In high-risk scenarios, additional personal information and supporting documentation may be requested to ensure sufficient identification and risk mitigation.

All Customers must be at least 18 years old and can only have one Player account in their name, as specified in Article 4 of the Conditions to Curaçao Online Gaming License. Therefore, no minors can play on the website. Furthermore, users who do not have a registered Player account will not be allowed to play.

6.3.8. Email Verification

When a new account is created, a verification link is sent to the email account specified during the registration process. When the user clicks on the link the account is then successfully created. Only at this point can the Player deposit money and start placing bets.

6.4. Customer Risk Assessment (CRA)

In accordance with section II.2.2 of the Curaçao AML/CFT Regulations, the Company performs a Customer Risk Assessment (CRA) for each Player to determine the level of risk they pose. The

Carletta N.V. – Anti-Money Laundering Compliance Policy

results of this assessment guide the application of customer due diligence (CDD) and monitoring controls, based on predefined risk categories.

The Customer Risk Assessment (CRA) is a formal, governance-level component of the Company's AML/CFT framework and, together with the Business Risk Assessment (BRA), is subject to periodic review and approval by the Board of Directors.

The CRA methodology, underlying risk indicators, and classification outcomes shall be reviewed at least annually – or sooner if regulatory, operational, or market developments require – and any amendments shall be submitted to the Board for formal approval.

Carletta N.V. shall maintain complete CRA and BRA documentation, including all updates and historical versions, and shall make such records available to the Gaming Control Board (GCB) immediately upon request.

The Company classifies Customers into Low, Medium, High-risk levels, and PEPs based on a numerical risk score generated during onboarding and ongoing monitoring. The Customer's score is calculated using weighted risk indicators covering five categories: customer profile, geographic location, product usage, delivery channel, and transaction behavior. These indicators and their associated scores are defined in **Annex B – Trigger-Based Risk Scoring Table**. The table below provides typical examples used in the classification process:

Carletta classifies Customers as follows:

Risk Score	Risk Classification	Applied Measures	Referenced Sections
1	Low Risk	Standard (or in some cases Simplified) CDD + Level 1 Controls	6.5, Annex B
2	Medium Risk	Standard CDD + Level 2 Controls	6.5, Annex B
3	High Risk	Enhanced CDD + Level 3 Controls	6.5, Annex B
PEPs	PEP (Separate Category)	Enhanced CDD incl. SoF/SoW, Management Approval + Level 4 Controls	6.5, 6.6, Annex B

a. Low Risk (Risk score 1)

Carletta N.V. – Anti-Money Laundering Compliance Policy

Customers with a low-risk rating will need to undergo basic customer due diligence (as described in the Customer Due Diligence Procedure) when reaching the established threshold of XCG 4,000 or on the first withdrawal. The Customers classified as low risk will be monitored at a lower rate. Based on changes in the Customer's behavior or risk profile, they may be reclassified to a higher risk category.

b. Medium Risk (Risk score 2)

Customers with a medium risk score will need to undergo standard customer due diligence (as described in the Customer Due Diligence Procedure) when reaching the established threshold of XCG 4,000 or on the first withdrawal. The Customers classified as medium risk will be more stringently monitored (as opposed to low-risk Customers), and Level 2 account controls will be implemented. Specific enhanced due diligence will be applied if specific risk indicators are identified.

c. High Risk (Risk score 3)

Customers with a high-risk score will need to undergo enhanced customer due diligence (as described in the Customer Due Diligence Procedure) when reaching the established threshold of XCG 4,000 or on the first withdrawal. The Customers classified as high risk will have the highest level of stringency applied to their ongoing monitoring. Level 3 account controls will be implemented. Full enhanced due diligence will be applied.

d. PEPs

PEPs (Politically Exposed Persons) will be classified as their own category and will receive exceptionally stringent attention and monitoring. All Customers that classify as PEPs will need to undergo compulsory due diligence as well as full enhanced due diligence including proof of wealth as well as proof of funds. Senior Management approval shall be required prior to establishing or continuing a business relationship with a PEP. PEPs will have the highest level of stringency applied to their ongoing monitoring. Level 4 account controls will be implemented.

6.5. Customer Due Diligence

The process of carrying out due diligence is three-fold: Simplified, Standard, and Enhanced Customer Due Diligence.

6.5.1. Simplified Due Diligence

This is the first stage of the process, which is carried out to identify and verify the Player.

Registered details will be cross-checked against any documentation and public information, including confirmation of the name, surname, date of birth, and address of the Player. Such documents requested by the Company may be in the form of scanned documents such as scans of the ID card or passport to confirm their identity. In instances where the ID card does not also confirm the Players' residence because no such residential information is provided on the document, then, a recent bill to confirm their address will be requested. This process may be kicked in upon registration or the first deposit phase but does not become a requirement until the thresholds are reached. In this stage verification of the source of wealth and source of funds will not require an in-depth analysis of the origin of the Customer's funds and the activities which have led to the accumulation of the Customer's wealth as the risk of ML/TF/FP is relatively low. At this stage, information regarding sources of funds or wealth is not required unless the Customer's risk profile changes or new risk indicators are identified.

6.5.2. Customer Due Diligence

This is the standard process that is to be followed for most of the customer base, provided they fall within the respective risk categories requiring the application of CDD. In addition to verifying the Customer's identity and residential address, date and place of birth, nationality, and identity number (where applicable), Carletta N.V. must also identify and verify the Customer's source of wealth. The Customer's source of wealth may be requested where appropriate, such as in higher-risk cases. The Company must be satisfied with sufficient certainty that the Customer has provided the necessary supporting documentation which proves the origin of the Customer's wealth and the activities that have led to the accumulation of the Customer's wealth effectively. The Customer will be allowed to deposit and make use of the Company's products but will not be allowed to make any withdrawals until such time as the documentation is received. If such documentation is not received within 30 days from when the Company requested such information and documentation from its Customers, the Customer's account shall be suspended, and the Customer will be precluded from depositing and making use of the Customer's products and services in addition to not allowing withdrawals to be made. A report should be sent to the Compliance Officer within 24 hours of the occurrence of such an event. The Compliance Officer shall then investigate and determine whether an UTR is to be filed with the FIU.

6.5.3. Enhanced Due Diligence

This is the third and most crucial stage of the due diligence process, as further information in terms of the Player is acquired. Such information includes acquiring sound knowledge and the respective supporting documentation to confirm the proof of source of wealth of the Player. This would include a higher level of staff with relevant experience, as such a process requires judgment when receiving such documentation and information from the Player. Upon any single or cumulative transaction, be it a withdrawal of any amount or deposit by any Customer amounting to XCG 4,000

Carletta N.V. – Anti-Money Laundering Compliance Policy

or more, the Player may be required to send proof of funds as part of the enhanced due diligence, depending on the associated risk indicators.

No further transactions may be processed until these documents are sent by the Customer and are checked and verified by the management.

This process is in line with Regulations to lower the AML risks. Upon registering a new Customer, his/her transactions and betting behavior will be checked and monitored daily. Mechanisms are in place that enforce a one-account-per-person policy, and if an issue of multiple accounts is detected, all relative accounts are suspended/frozen until the matter is resolved. Scripts are in place that detect strange or unusual behaviors from our Customers, and our software provider partners are immediately notified. This procedure enables the Company to analyze the way every individual uses the products from our website, making it possible to categorize the Players and thus set limits on the individual Players according to their betting habits.

6.5.3.1 Beneficial Ownership and Third-Party/Syndicate Funding Controls

Carletta N.V. does not onboard corporate or legal-entity Customers and provides gaming services exclusively to natural persons. Nevertheless, in accordance with Curaçao AML/CFT Regulations, the Company must identify, assess, and mitigate situations in which a Player account is directly or indirectly funded by a third party, including corporate entities or coordinated groups (“syndicate funding”).

The Company prohibits the use of corporate bank accounts, corporate cards, business wallets, or any payment instrument registered to a legal entity for the purpose of funding a Player account. Where a deposit, attempted deposit, or payment instrument is identified as belonging to a company or other legal entity, the transaction shall be rejected and escalated to the Compliance Officer for review.

If the Compliance Officer determines that funds may originate from a legal entity or a pooled/syndicated arrangement, the Company shall:

- identify and verify the natural persons who ultimately own or control the funding entity (Beneficial Owners/UBOs), where such information is necessary to assess AML/CFT risk;
- apply Enhanced Due Diligence measures, including verification of source of funds and source of wealth;
- restrict or suspend the account pending completion of the assessment;

- submit an Internal Suspicion Report (ISR) where appropriate.

Coordinated group funding, shared banking instruments, or the use of multiple third-party payment methods inconsistent with the Player's profile constitute prohibited activity. Any indicators of such syndicate or third-party funding scenarios shall trigger EDD, account restrictions, and – where applicable – an Unusual Transaction Report (UTR) to the FIU.

Where a Player account is funded by another natural person, or where there is reason to believe that the Player is acting on behalf of another individual, the Company shall identify and verify the Beneficial Owner of the funds. This includes situations where deposits, payment instruments, or gaming activity indicate third-party financing, sponsorship, or proxy use by another natural person. In such cases, EDD shall be applied, including verification of the identity, source of funds, and relationship between the parties.

6.5.4. Customer identification and verification guidelines

To make a first deposit with Carletta N.V. a Customer needs to provide the following mandatory details:

- First name
- Last name
- Street and street number
- City and postal code
- Country
- Email address (must be valid and unique within Carletta N.V.)
- Date of birth
- Place of birth
- Nationality
- Password (will be encrypted)
- Confirmation of password
- Account currency
- Mobile phone number

A newly registered Carletta N.V. account will be checked in the shortest time possible by the service department to find out if the details are correct (accounts with fake names and addresses will be closed). Also, the registered country and the IP-country address need to be compared. A mismatch is automatically flagged in the Customer's account. This helps the Company to close fake accounts before any pay-in can be processed.

Carletta N.V. – Anti-Money Laundering Compliance Policy

Players who are not registered are unable to play for real money. Any online transaction, may it be a pay-in or payout, will not be accepted or processed.

To determine the initial risk profile the following checks are also performed regarding each Customer:

- Politically Exposed Person (PEP) screening;
- Sanctions Lists Screening.
- Geo-Location

Once the registration process has been finalized, Customers will receive a welcome email with a link to access their accounts. This procedure aims to verify the Customer's email address.

Before reaching one of the specified thresholds (XCG 4,000 total deposits, first withdrawal request, suspicion of ML/TF/FP), customers go through an initial Risk Assessment screening in order to determine if the Customer's risk profile falls within the Company's risk appetite. The following pieces of information are checked regarding each Customer in order to determine the initial risk profile:

- Funding Methods
- Requested Product Type(s)
- Business Relationship Channel

Each new Customer must provide a copy of an ID document (passport, ID card, or driving license) when relevant thresholds are reached. This is in line with the local transposition and implementation of the AML/CTF measures.

The identity check has to include a copy of a utility bill and/or bank statement showing the name and address and cannot consist of a mobile telephony bill.

Furthermore, the identity check may include additional measures such as the provision of a copy of each credit card used in the specific account. Further details can be found in the Procedure detailing the Due Diligence process.

Any remaining doubts concerning the identity of a Customer have to be reported based on the Procedure detailing reporting lines. In such a case, further investigations have to be started.

These may include:

- Check the IP used by the Customer
- Check the provided phone number and/or call the provided phone number
- Internet research on the Customer details
- Request to the official authorities in the country of the Customer – this has to be done by compliance management.

These steps are further described in the Company's documented CDD procedures.

The due diligence criteria are set as follows:

- ID documents must be official documents issued by a government entity that include confirmation of the name and residential address, or date of birth, and a photo, such as a passport, can be used to verify an identity. Where this type of documentation is not available, a government-issued document confirming the name of the individual and supporting document supplied by a public authority, court, or a financially regulated service provider that includes the individual's full name and either date of birth or residential address can be used.
- The details in the passport are compared to other documents collected at the Company's discretion.
- When in doubt of forgery, the Player is requested to hold up the passport to his/her face to verify that such passport belongs to the said individual.
- Online public databases are checked to cross-check the information in the documents provided.
- Public searches through social media and other sources are checked to build the Player profile.
- Finally, if it comes to our attention that the individual is a politically exposed person, enhanced due diligence is immediately carried out, and the account is monitored closely.
- If the Customer comes from a high-risk jurisdiction, the enhanced due diligence process is kicked off immediately, and the account is monitored closely. It is at the operator's discretion to refuse registrations from high-risk jurisdictions.

6.5.5. Sanction List Screening

The Company shall conduct sanctions screening upon Customer registration and, where appropriate, periodically thereafter based on the Customer's risk profile, in line with its obligations under the Sanctions National Ordinance, the Kingdom Sanction Act, and the FIU implementing procedures, respectively.

Upon registration, the Customer will be screened against the consolidated sanctions list issued by the United Nations Security Council (UNSC)¹ and the European Union (EU)², as required by Curaçao's legal and regulatory framework. Additional screening against other internationally recognized sanctions lists — such as those maintained by the U.S. Office of Foreign Assets Control

¹ UN Sanctions List: <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

² EU Sanctions List: <http://www.sanctionsmap.eu/#/main>

Carletta N.V. – Anti-Money Laundering Compliance Policy

(OFAC)³, or other relevant bodies — may be conducted at the Company's discretion, particularly in the context of enhanced due diligence (EDD).

Such screening will then be conducted periodically based on the Customer risk assessment conducted. The frequency of such sanction list screening will be increased should a Player reach the XCG 4,000 threshold, although such frequency will still be determined according to the Customer's risk. Moreover, the frequency of such screening will also be impacted by the PEP status of the particular Player.

If the Company becomes aware that one of its Customers, or potential Customers, is subject to an international Sanction, or has ties to countries or entities subject to such sanctions, the Company must immediately inform the FIU without delay. All appropriate measures must be taken to ensure that any assets, including funds held on behalf of such individuals, are frozen immediately until further instructions are given by the FIU.

For more information on jurisdictional risk classifications, including prohibited countries, high-risk, medium-risk, and standard-risk jurisdictions, please refer to **Annex C - Jurisdiction Risk Classification and Prohibited Countries List**. This annex outlines:

- Countries prohibited for registration or access due to regulatory restrictions or inclusion on sanctions lists;
- High-risk jurisdictions, including those listed by FATF and OFAC;
- Medium-risk jurisdictions identified based on the Transparency International Corruption Perceptions Index (CPI);
- All other jurisdictions not explicitly listed above, considered standard-risk unless otherwise assessed.

6.5.6. Player Verification Procedure

Players will be requested to provide mandatory due diligence documents during the following stages:

- Prior to the Player reaching the XCG 4,000 deposit threshold
- Upon request for the first withdrawal
- At any other stage, the Company's systems or employees detect any suspicious/unusual behavior of the Player or have any doubt on the accuracy of the information provided during the Registration Process or a Player Account classified as High Risk.

Players are obliged to provide the Company with documents that verify their identity and address.

³ OFAC Sanctions List: <https://sanctionslist.ofac.treas.gov/Home/SdnList>

The Company's employees should oversee this procedure and, where any red flags are raised or registration has been rejected and are unable to complete the registration process, the employees should manually review the documents provided and the reasons for rejection. In such cases, the employees should thoroughly check all the documents provided and third-party verification reports, and reconsider whether the documents should be accepted or rejected, and in case of rejection, whether to request the Customer to provide new and/or additional documents or suspend the account and report the case to the Compliance Officer in line with the Company's internal reporting procedures.

The Company's employees, in terms of the Player verification process, shall review the following documents:

- Documents needed to verify Players' identities:

A clear, color, scan, or photo, alongside a selfie picture of any of the following:

- Official ID card (both sides)
- Passport (open and display the full photo ID page of the passport holder)
- Driving License (both sides)

- Documents needed to verify the Players' address:

The Player should provide a clear scan, color photo, PDF, or screenshot of any official document addressed to them, issued within the last 6 months, stating their full name and current address. This can include one of the following:

- Utility bill (electricity, water, gas, landline phone bill, internet line account)
- Bank statement or reference letter
- Credit card statement
- Tax/welfare letter
- correspondence from a central or local government authority, department or agency, or any other government-issued document.

- Any additional documents:

At any stage, Players may be asked to provide any further information to those already provided or any additional documentation (check Annex B), at the Company's sole discretion.

Upon receiving the required documents and for the Player's account to be validated, the Company's employees shall conduct a manual check on the information/documentation received and consider whether more information/documentation is needed. The following checks are to be performed:

- Check whether the Player's personal data listed in the document provided matches the information provided during the registration
- Cross-checking of any third-party report on similarity checks and whether the Selfie meets the system requirements (clear photo of the Player's entire face without wearing glasses,

Carletta N.V. – Anti-Money Laundering Compliance Policy

hats, scarves, or any other accessory that covers the face, in whole or in part) has been adhered to

- Make sure that the system does not allow registration of Players who are underage (according to clause **6.5.7. Applied Due Diligence Measures and Account Controls Breakdown, Protection of Minors**), coming from restricted countries, or have another Player Account in their name.
- Manual check of documents provided to verify Players' address
- Verify the validity and authenticity documents provided
- Verify and confirm that the documents provided contain all necessary information, according to the information it is meant to verify

6.5.7. Applied Due Diligence Measures and Account Controls Breakdown

Based on the customer risk class, specific control levels will be applied to each customer account to mitigate the inherent risk posed by any of these classes. The controls will be applied based on which risk criteria are more relevant when calculating customer scores. The list below is by no means exhaustive and Carletta N.V. employees will seek guidance and advice regarding specifically suspicious accounts and situations from middle management, the compliance department, the Compliance Officer, and Senior Management when the need for more stringent controls arises.

a. Level 1

- Proof of ID
- Proof of address
- Proof of funds (where applicable)
- Copy of Credit card (where applicable)

b. Level 2

Controls may include but are not limited to:

- All controls mentioned for Level 1 above
- Proof of Source of Wealth
- Proof of Source of Funds

c. Level 3

Controls may include but are not limited to:

- All controls mentioned for Level 2 above
- Secondary proof of address
- Certified copies of due diligence documentation
- Video call with Customer for verification purposes
- Professional/Bank Reference Letters

d. Level 4

Controls include but are not limited to

- All controls mentioned for Level 3 above
- Manual information review by Compliance Officer
- Management approval for relationship continuation
- Daily account monitoring by relevant teams

Carletta N.V. has multiple stages of Customer Due Diligence (CDD) in place to mitigate as many of the risks posed by the possibility of Money Laundering and Terrorist Financing as possible as well as properly understand their Customers as well as the nature of the intended business relationship.

To this extent, specific mechanisms have been put in place to:

- Determine who the Customers are
- Verify whether that person is the person he/she purports to be
- Determine whether a person is acting on his/her behalf or on behalf of another person
- Establish the purpose and intended nature of the business relationship and the Customer's business and risk profile
- In the case of a business relationship, monitor that relationship on an ongoing basis.

Carletta N.V.'s applied due diligence measures consist of the following:

- Identification and verification of the Customer
- Obtaining additional information on the purpose and intended nature of the business relationship
- Understanding and verifying the Customer's source of wealth and source of funds, where applicable
- Ongoing monitoring

Customer Due Diligence

Carletta N.V., following the Regulations, requests all Customers to provide standard due diligence in the following cases:

- Player reaches the threshold of XCG 4,000 as required by the GCA.
- Player requests their first withdrawal.
- Any reasonable suspicion towards the Player is raised.
- A change in the Customer's risk rating.

Standard due diligence contains but is not limited to the following documents:

- Proof of Identity – This documentation will be used to begin verification of Customer

Carletta N.V. – Anti-Money Laundering Compliance Policy

identity and will create the basis of the Customer's profile. The proof of identity might consist of but is not limited to a copy of a Local government-issued ID, a Copy of a Passport, a Copy of a Driver's License, a Copy of a Residency Card (where applicable).

- Proof of Address – This documentation complements the proof of identity and assures the Customer has their residency where they claim they do, so proper measures can be applied to cater to their specific jurisdiction requirements. The proof of address may consist of, but is not limited to Utility Bill, Lease Agreement, and Bank Statement.
- Source of funds – This piece of documentation is required in situations where a transaction or series of transactions is out of the ordinary or contrary to the estimated Customer rollover capacity per transaction or series of transactions. This is to ensure the funds used for an outstanding transaction or series of transactions have not been acquired by any predicate crime. Source of funds may consist of but is not limited to a letter from the bank explaining said funds, proof of sale (in case funds were obtained from the selling of movable or immovable property), a bank statement specifically showing the source of funds used, proof of ownership of any security, proof of ownership of any legal entity and its related financial statements, dividend warrants.
- Ongoing Monitoring – As per Regulation all Customers need to undergo ongoing monitoring to a certain extent based on risk profile. A less stringent monitoring regime will be applied to Customers that have scored below High Risk (for more details on risk levels please see **Sections 6.5–6.6 of this Policy**).

Enhanced Due Diligence

As per Policy all Customers that pose a high risk of ML/TF/FP, are politically exposed or it is determined that it will be more prudent to apply EDD measures, will be requested to provide extra documentation and proof of verification based on the most relevant risk factor(s). As described in the Onboarding Procedure each risk rating higher than low risk warrants a level of extra documentation, however, if deemed necessary one or more of the following actions will be taken to ensure the Customer is properly verified and the risk of ML/TF/FP is well kept under control. The following list describes the most common documents that can be requested for enhanced due diligence purposes. However, it is not exhaustive, and Carletta N.V. reserves the right to request any documentation to the point where management is satisfied with the Customer verification:

- Copy of Debit/Credit Card – this piece of documentation is requested to verify that the deposit means used is indeed under the correct name that was collected during the initial identification and verification procedure
- Bank Statement – this piece of documentation is requested in cases where money has been transferred using bank transfer and helps verify that the account used for the transfer is indeed under the name collected during initial identification and verification. The Bank Statement is also used as supporting documentation for the source of funds and wealth.
- Letter from the Bank – this piece of documentation is requested as further proof of the

- Customer's identity as well as to double-check his reputation with a financial institution.
- Certified True Copies of Due Diligence Documentation – certifying the copies of the required documents offers extra control towards the accurate verification of the Customer's identity using a secondary licensed person checking that the documents are veritable. This can be requested when there is suspicion that the documentation might have been tampered with.
 - Recorded Video Call – this action is taken when there are doubts that the person using the Carletta N.V. account is the one whose due diligence documentation has been received. Specific interactions are required on behalf of the Customer to make sure that the footage is live. This procedure is not meant to eliminate the risk posed by a non-face-to-face relationship which will still be taken into consideration when analyzing the Customer, however, it will provide extra assurance of the legitimacy of the Customer's claims.
 - Account Review by Compliance Officer – this action is taken when there is suspicion of ML/TF/FP towards the Customer but there is not sufficient information for filing an UTR. The Compliance Officer checks the account and gathers all needed information to make a final decision regarding the ML/TF/FP suspicion.
 - Senior Management Approval for Relationship Continuation – In cases where the Customer is a politically exposed person or otherwise poses a high risk of ML/TF/FP but does not raise any suspicion based on behavior or documentation, express approval from Senior Management will be required to continue the business relationship.
 - More Stringent Account and Transaction Monitoring – all accounts deemed as High Risk will be subject to more stringent scrutiny from the relevant teams.

Simplified Due Diligence

Such measures shall only be applied in low-risk scenarios, provided none of the other CDD or EDD thresholds are reached. In such a case Level 1 controls will be applied.

CDD: Player Limits and Limit Monitoring

Based on jurisdictional requirements Players may be required to set deposit limits upon opening an account with Carletta N.V. The Company's staff will make sure these limits are applied. If a particular Player sets their deposit limit higher than the approved amount, they will be contacted by the Company's relevant departments and will be requested to provide reasoning for their limits. Where any ML/TF/FP suspicions come up based on the Player behavior analysis, the case will be escalated to the Compliance Officer and an EDD requirement may be triggered.

Protection of Minors

Carletta N.V. – Anti-Money Laundering Compliance Policy

Prospective Customers under the age of 18 will be denied registering an account. Customers are required to register before playing for real money. Responsible gambling procedures are put in place to ensure persons under the legal gambling age are denied access to gambling services.

The registration process requires confirmation of date of birth, as well as confirmation that the Customer is over 18 years of age.

Should a Player still manage to go through the registration process and is in fact under the age of 18, the Company has implemented controls to check and verify the age and identity of the Customer. This includes requesting KYC documentation from the Player e.g. upon first withdrawal. Should at any stage the Player be found to be a minor, all stakes, winnings, and bonuses are to be forfeited, the deposit returned (at least, any part of it that remains), and the account blocked.

Politically Exposed Persons

1. The meaning of a 'Politically Exposed Person':

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refer to members of senior management, i.e. directors, deputy directors, and members of the board or equivalent functions.

Both domestic and foreign PEPs are to be considered as PEPs and EDD measures on a risk-sensitive basis must be applied.

2. Persons known to be close associates include the following:

- (a) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in point (4) above;
- (b) any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in point (4) above.

The Company shall apply the following to the accounts of “Politically Exposed Persons”:

1. The establishment of a Business Relationship or the execution of an Occasional Transaction with persons holding important public positions and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Customer seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate family or a close associate of or is known to be associated with a PEP.

The Company shall pay even more attention when the said persons originate from a country that is widely known to face problems of bribery, corruption, and financial irregularity and whose anti-money laundering laws and regulations are not equivalent to international standards or who have been flagged as having regulatory deficiencies by the FATF or any other regulatory and/or monitoring authority.

2. To effectively manage such risks, Carletta N.V. shall assess the countries of origin of its Customers to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40 recommendations of the FATF.

Country risk assessments may include reference to public indices such as FATF country evaluations. As part of its country risk assessment process, the Company may also refer to internationally recognized indices, such as the Transparency International Corruption Perceptions Index (CPI), to assess the level of perceived corruption in a jurisdiction.

Concerning the issue of adequacy of application of the 40 recommendations of the FATF, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating by FATF’s principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

3. Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, the Company shall not be automatically obliged to consider a person as PEP solely due to their previous public function, if a significant period of time has passed since the individual ceased to perform that function. However, the Company may still consider such a person to be a PEP based on the risk associated with their former role, influence, and exposure.
4. Without prejudice to the provisions of this document, Carletta N.V. will adopt the following additional due diligence measures when it establishes a Business Relationship or will carry out an Occasional Transaction with a PEP:

Carletta N.V. – Anti-Money Laundering Compliance Policy

- (a) Carletta N.V. puts in place appropriate risk management procedures to enable it to determine whether a prospective Customer is a PEP. Such procedures may include, depending on the degree of risk, the acquisition, and installation of one or more reliable commercial electronic databases for PEPs, seeking and obtaining information from the Customer himself or publicly available information. In the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorized signatories, and persons authorized to act on behalf of the legal entities and arrangements constitute PEPs. In the event of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Policy.
 - (b) The decision to establish a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by the Senior Management of the Company and the decision is then forwarded to the Compliance Officer. When establishing a Business Relationship with a Customer (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then approval is given for continuing the operation of the Business Relationship by the Senior Management of the Company which is then forwarded to the Compliance Officer.
 - (c) Before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the Company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. using publicly available sources, including open media, corporate registries, and sanction or watchlists.).
 - (d) Carletta N.V. shall create the economic profile of the Customer by obtaining the information specified in Sections III.4 and III.6 of the Regulations. The profile shall be regularly reviewed and updated with new data and information. The Company shall be particularly cautious and most vigilant where its Customers are involved in businesses that appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes, and alcoholic drinks.
 - (e) The account shall be subject to a shorter review period than would otherwise be assigned for a Customer of a similar risk, to determine whether to allow its continuance of operation. Such a period shall take into account the position and measure of political influence the PEP has as well as the inherent risk and mitigating measures associated with the products being offered to such a Customer. An Internal Report shall be prepared summarizing the results of the review by the person who oversees monitoring the account. The report shall be submitted for consideration and approval to the Partners and filed in the Customer's file.
 - (f) Carletta N.V. is required to obtain a higher standard of the quality of documents obtained.
5. The Company will carry out or, in the case of applying enhanced ongoing monitoring, implement these measures at any point in time between the establishment of the Business Relationship and the point in time when the XCG 4,000 threshold is met, but not later from the

lapse of thirty days from when the said threshold is reached. In the case of an Occasional Transaction, the Company will carry out the said measures, in so far as they are applicable, before carrying out the transaction in question.

6. Screening for PEP status will also be carried out regularly during the business relationship. Should a Customer who had not been identified as a PEP at the onboarding stage result to have become one, the licensee concerned has to carry out or obtain senior management approval to service the PEP as well as establish the source of wealth and, where applicable their source of funds is within the thirty-day window, failing which it would have to terminate the business relationship with the said Customer as described in Section III.6 of Regulations.
7. The Company shall monitor the PEP registers to better ascertain if potential or current Customers are PEPs or whether any officials or related personnel of a Customer are PEPs. Such registers are to be considered as guidance tools, and one should always endeavor deeper to determine whether a person is to be considered as a PEP.

Carletta N.V. is aware of its duties towards identifying and carrying out due diligence in terms of politically exposed persons.

6.6. Ongoing monitoring

The Player risk profile is a document describing the various items taken into consideration, when enough information is gathered regarding a Player, to determine the risk said Player poses to the Company from an AML/CFT perspective within the confines of the Business Risk Assessment (BRA) created for the Company.

The Player risk assessment is created in one of the following situations:

- Player reaches the required threshold (XCG 4,000)
- Player makes their first withdrawal
- Suspicion has been raised internally regarding the Player's activity
- Change in Customer's PEP status
- Increase in Customer risk classification

In either of the above-mentioned cases, a Player risk profile is drafted and filled in using information gathered during the Business Relationship. Should additional control measures be applied, the response, information, and documentation provided shall also be taken into account when drafting such a Player risk profile.