

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 Shehikovskii – Compliance Officer	Fesilia Vivian Victoria, (SMES) Solution for Management and Employment Support N.V. – Director	Initial Release	May 27, 2025	
			Next Review	May 27, 2026	

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)	22
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	23
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.....	26
6.5.3.	Enhanced Due Diligence	27
6.5.4.	Customer identification and verification guidelines	27
6.5.5.	Sanction List Screening.....	30
6.5.6.	Player Verification Procedure.....	31
6.5.7.	Applied Due Diligence Measures and Account Controls Breakdown	32
6.6.	Ongoing monitoring	40
6.6.1.	The customer risk profile contains the following fields	40
6.6.2.	Format of Records.....	44
6.6.3.	Certification and language of documents.....	44
6.6.4.	Procedures.....	44
6.6.5.	Timeframes	45
6.6.6.	Payout Management Procedure.....	46
6.6.7.	Dormant Accounts.....	48
6.7.	Reliance on Third Parties to perform Customer Due Diligence	48
6.8.	Unusual Transaction Reporting.....	48
6.8.1.	Internal reporting and escalation procedure.....	49
6.8.2.	Knowledge.....	50
6.8.3.	Compliance Officer's report to the FIU	51
6.8.4.	Submission of information to the FIU	51
6.9.	AML Compliance Program	52
6.10.	Record keeping and monitoring.....	53
6.11.	Independent audit.....	54
6.12.	Examination by the Curaçao Gaming Authority (CGA).....	55
7.	AML GOVERNANCE & RESPONSIBILITIES.....	55

8. EMPLOYEE TRAINING PROGRAM	59
8.1. Employees' obligations	59
8.2. Employees' Education and Training	59
8.3. Compliance Officer Education and Training Program	60
9. CONSEQUENCE OF NON-COMPLIANCE (NOIS and NORUT)	61
9.1. Sanctions for Non-Compliance	61
9.2. Personal Liability of Responsible Officers	61
10. AGENTS/INTERMEDIARIES	61
11. RELATED INFORMATION	62
12. CONTACT INFORMATION	62
ANNEX A - Internal Control Structure: Three Lines of Defense	63
ANNEX B - Trigger-Based Risk Scoring Table	65
ANNEX C - Jurisdiction Risk Classification and Prohibited Countries List	68
ANNEX D - Standardized template of the Internal Suspicion Report (ISR)	71
ANNEX E - Annual AML/CFT Training Plan	73
ANNEX F - Examples of unusual transactions/activities related to money laundering and terrorist financing	75
ANNEX G - Employee screening program	78
ANNEX H - Responsibilities of the Compliance Officer as required by the CGA	79
ANNEX I – Ongoing employee training program	80

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.

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;
- 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 FATE, 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 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 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 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, 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 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.

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).

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).

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 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.

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.

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 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.

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

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:

Carlitta 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)

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 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.

6.5.4. 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.

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 (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;

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

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

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

- 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. 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, 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 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/FT/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

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:
 - (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.

6.6.1. The customer risk profile contains the following fields

Username as stored in the back office

When creating an account with the Company the Player selects a username that will be stored within the Company's back office and is used to further identify the Customer. The username itself cannot be utilized to identify the Customer unless access is provided to the secured Company back office and thus anonymization is achieved to satisfy personal data privacy standards/requirements.

Access to personal and risk-related data is restricted and managed in accordance with the Company's internal data protection and security policies. Any linkage between a Player's risk profile and their personal identifiable information is subject to appropriate access controls, ensuring compliance with applicable data protection laws.

Funding method as described in the back office

The Company's back office stores all possible funding methods for all jurisdictions within its back office and allocates these funding methods to Players using them accordingly.

Each funding method contributes to the Player's overall Customer Risk Assessment (CRA) score, in line with the Company's Risk-Based Approach (RBA) and the findings of the Business Risk

Assessment (BRA). Players using high-risk payment methods may be subject to Enhanced Due Diligence (EDD) or rejected under the Customer Acceptance Policy (CAP) if their total risk score exceeds the permitted threshold.

Each payment method has received an internal relevant risk score based on the strength of the controls applied to the Customers using said particular payment methods, as well as on the strength of the AML policies and procedures employed by the payment method providers themselves.

The risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	1	• European or EU equivalent bank transfers • Debit cards issued by credit institutions within the EU/EEA or at EU standards
Medium	2	• EU/EEA Credit Card • EU/EEA PSP which does not allow Customers to fund with cash or quasi-cash
High	3	• Prepaid Cards • Vouchers • NON-EU/EEA Debit card • NON-EU/EEA Credit card • VFAS (cryptocurrencies) • EU/EEA licensed payment providers that can be funded with cash or quasi-cash • Non-EEA licensed PSPs that allow Customers to fund with cash or quasi-cash • NON-EU/EEA which do not allow Customers to fund with cash or quasi-cash.

NOTE: Some of the risk categories found in the above ratings might not be currently present within the Company's risk appetite, however, they have been noted in the general risk assessment as to be used at any future date in case the Company deems it necessary.

The current payment methods have been adjusted to reflect the status of the Company's risk appetite in the individual scores.

Player Jurisdiction

The Company takes into consideration Player jurisdiction upon onboarding to ensure that the country the Player comes from is within the Company's risk appetite.

All countries accepted by the platform have been analyzed based on the individual controls applied by the Company on a case-by-case basis, as well as concatenating information from various online resources that offer insight into the risk specific jurisdictions pose from an AML/CFT perspective.

Each country supported by the platform has been given a risk score based on the data processed from the various resources.

Please refer to **Annex C - Jurisdiction Risk Classification and Prohibited Countries List** for the main documentation used for determining a country's risk rating.

The jurisdiction risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	1	Countries that offer a strong AML/CFT regulation in line with international standards. Countries that offer good AML/CFT regulation and show signs of constant improvement
Medium	2	Countries that offer an acceptable AML/CFT regulation have shown plans to improve in the future. Countries that offer a baseline AML/CFT regulation and controls can be put in place to mitigate risks
High	3	Countries lacking sufficient and/or effective AML/CFT regulation and controls in place to mitigate risks
Blocked/Extreme	N/A	Countries banned via platform to avoid risks from an AML/CFT perspective and countries listed as High-Risk Jurisdictions subject to a Call for Action by the FATF

Player registration channel

The Company offers the possibility of online registration for its Players. Upon registration, Players must provide core identifying details such as full name and date of birth, in accordance with the Company's onboarding and identification procedures. Once the Player deposits and starts to wager, the account is monitored for any increase in risk or high-volume wagering/high amount wagering. Should it be deemed necessary, the Customer will be asked to verify the source of funds

even though the relevant thresholds have not been met. Should it transpire that the information and documentation provided at this stage is fake, inaccurate, or incorrect, the account will be suspended, and an investigation will be initiated to determine whether there are sufficient grounds to file an UTR.

Player first deposit amount

The Company considers that the initial sum deposited by a specific Player is crucial in determining the type of behavior the Company needs to exhibit toward the Player from both an AML perspective as well as a Responsible Gambling perspective.

To this extent, the possible first deposit amounts have been broken down into 3 categories beginning with the most common deposit amount and incrementing to the threshold for due diligence requirement.

The deposit amounts are broken down as follows:

Risk Rating	Risk Score	Amounts (XCG)
Low	1	0 to 2,000
Medium	2	2,001 to 4,000
High	3	4,000 +

Player first withdrawal amount

The Company monitors the initial withdrawal amount to determine the type of business relationship the Customer seeks to form with the Company as well as to place monitoring flags on the Customer account for future withdrawal actions and search for any suspicious patterns.

The withdrawal amounts are broken down as follows:

Risk Rating	Risk Score	Amounts (XCG)
Low	1	0 to 2,000
Medium	2	2,001 to 4,000
High	3	4,000 +

6.6.2. Format of Records

The Company's Management shall retain the documents/data mentioned in this Policy, other than the original documents or their certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Company's Management shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to the FIU or any other relevant authority, after a relevant request.

In case the Company establishes a documents/data retention policy, the Compliance Officer shall ensure that the said policy shall take into consideration the requirements of the Law and the Directives.

The Internal Auditor shall review the adherence of the Company to the above, at least annually.

6.6.3. Certification and language of documents

The documents/data obtained shall be in their original form or as a copy of the original. In high-risk cases or if deemed appropriate, the Company may request documents to be certified as true copies of the original and/or be apostilled. In the case that the documents/data are certified as true copies by a different person than the Company itself or by the third party with whom a reliance and or intermediary agreement has been reached, the documents/data must be apostilled or notarized or certified by a professional whose identity and professional capacity must be confirmed and verified. In certain high-risk cases, identification and verification of the certifier may also be necessary.

A true translation shall be attached in the case that the documents mentioned above are in a language other than English, or a language which is not known by the person reviewing the document.

6.6.4. Procedures

The procedures and frequency relating to the monitoring of Customers' profiles, accounts, and examination of transactions based on the Customer's level of risk shall include the following:

(a) the identification of:

- transactions which, as of their nature, may be associated with money laundering or terrorist financing.
- unusual or suspicious transactions that are inconsistent with the economic profile of the Customer for further investigation.

- in case of any unusual or suspicious transactions, the administrator handling the specific Customer as well as the Head of that Department shall be responsible for communicating with the Compliance Officer.
- (b) Further to point (a) above, the investigation of unusual or suspicious transactions by the Compliance Officer. The results of the investigations are recorded separately and kept in the file of the Customers concerned.
- (c) the ascertainment of the source and/or origin of the funds credited to accounts.
- (d) the use of appropriate IT systems.
- (e) For the Company to comply with its monitoring requirements it shall review the Customer's file according to the timeframes, as per section 5.15.3 below, and take into consideration the following to assess whether any additional or replacement documentation/evidence might be required:
- Update any expired identification documentation
 - Update any changes in the companies' structure and involved people.
 - Changes in the Customers' activities which might have an impact on the Customers' economic profile.
 - Reviewing ways in which new products and services may be used by criminals for money laundering and/or terrorist financing purposes, and how these ways may change to conceal such illicit activities.
 - The compliance officer performs checks to ensure that the relevant reviews take place and documentation is kept accordingly.
 - Reporting and accountability by the compliance officer to the Board of Directors and Senior Management.
 - Liaising with the Curacao Gaming Control Board, FIU, or any other relevant/applicable authority in a case where such liaising is required.

6.6.5. Timeframes

The time frames set below shall act as guidelines for the Compliance Officer when setting the dates for the re-review dates. Such time frames may be changed if justified notwithstanding the Customer has been risked as in a category, provided such justification is recorded. Furthermore, these time frames should be changed and updated should any of the factors affecting the risk the Customer poses change. The below time frames shall be taken as guidance points and not as a mandatory rule.

Risk Classification	Time Frames
Low Risk	12 - 24 months
Medium Risk	6- 12 months
High Risk	3 - 6 months

6.6.6. Payout Management Procedure

Checks to be performed on each pay-out:

a. Account check

The owner of the Carletta N.V. account must be the same person as the owner of the bank account or credit card. All account information, like address, email, date of birth, etc., must be complete and authentic. Withdrawals will be made to the same source where the funds originated (where possible).

b. Deposits must have been used

On each payout, the Company will verify whether the deposits have been used for stakes. All deposit amounts need to have been wagered at least once (1) when a bonus was not credited before a withdrawal request can be made. In the case where a bonus has been utilized, the total amount of deposit and bonus must be wagered at least seven (7) times before being allowed to make a withdrawal. A pay-out cannot be processed if the deposited amount has not been used for stakes. With reference to the second sentence in this paragraph, if the deposited amount has not been used, the payout has to be denied. Furthermore, the latest winnings have to be checked for correctness.

c. Fulfilment of bonus rules

Before a payout can be deducted from the Customer's account, the account has to be checked if a bonus has been given to the Customer since the last payout. When a bonus has been credited, the account has to be checked for the fulfilment of the bonus rules applicable to that bonus.

If bonus rules have not been fulfilled the requested pay-out cannot be completed.

d. Deposit of funds

Funds deposited in the gaming wallet can only be used for gaming activity. Should Carletta N.V. notice regular changes by Players to the payment method linked to the gaming wallet, the account will be suspended until the necessary explanations are provided by the Player for these changes.

Carletta N.V. does not allow Players to transfer funds between accounts under any circumstances.

The Company's KYC team continuously monitors Players' deposit activity as well and has automated processes in place to receive notifications when Players achieve the XCG 4,000 (four thousand) transaction limit.

e. Risk Profile for Carletta N.V.

The risk profile and risk appetite for Carletta N.V. will be calculated based on the Business Risk Assessment done at a minimum once every year. The Business Risk Assessment will take into consideration all risks the Company faces constantly as well as the mitigating factors controlling the inherent risk. Modifications will be done to the policies and procedures for Carletta N.V. based on the resulting risk, as soon as the need arises.

Withdrawals can only be paid to the same Customer's account used to deposit money. This is in line with p. III.8. of Regulations, which provides that there is a higher transaction risk if the user's card is issued in the name of third parties. Therefore, the funds to be paid to the Player can only be withdrawn to the same account from which the funds paid into the Player's account originated. If the payment method used does not allow Carletta N.V. to settle payouts to the same payment method, then Carletta N.V. must identify and verify that the method used to settle the withdrawal request belongs to the Player in question.

Carletta N.V. does not accept cash from Customers, and funds may only be received through online transfer. In the same manner, no withdrawals can be processed as cash. Withdrawals will always be remitted to the same account from where the funds originated or to an account or payment method that has been verified as belonging to the Player.

At all times Management shall ensure that the total of all the Players' account funds including any funds in transit shall be at least equal to the aggregate of the amount standing to the credit of the Players' accounts held by the Company to have sufficient funds to pay out the prize money with appropriate ring-fencing and segregation measures as prescribed by per p.5, Art.6 of the Conditions to Curaçao Online Gaming License.

CDD documentation is always requested and verified for all Players affecting a single or cumulative (e.g. in one day) transaction of XCG 4,000 or more or upon requesting to withdraw funds.

The system will automatically stop minors from registering as Players inputting a date of birth below the age of 18 years of age.

6.6.7. Dormant Accounts

If a Player does not log in to his/her Player Account for 180 consecutive days, it will be classified as an "inactive account." The Company will notify the Player via email at least 30 days before the account becomes inactive. Once an account is deemed inactive, the remaining balance will be debited from the account. Following the account becoming inactive, the Company will suspend the account at that time for security reasons. This means that following the Player's request and following completion of any identity verification checks, the Company will restore access to the account. Funds that were debited due to the account suspension are not subject to a refund.

6.7. Reliance on Third Parties to perform Customer Due Diligence

Carletta N.V. relies on the services of **KYCAID LIMITED**, a qualified third-party KYC provider, to conduct specific onboarding and customer due diligence (CDD) activities. These include identity verification, document validation, biometric checks, and sanctions/PEP screening.

Further information regarding the responsibilities of third-party providers and the first line of defense can be found in Section 6.2.8. **"First Line of Defense (KYC and Onboarding Staff)"** and Annex A **"Internal Control Structure: Three Lines of Defense"**.

6.8. Unusual Transaction Reporting

In any case, where the Company encounters, verifies or there exists a reasonable suspicion that any form of money laundering is taking place or being attempted, such activity or transaction will be reported to the Financial Intelligence Unit (FIU), as required. The activity or transaction will be reported through the portal for filing and submitting Unusual Transaction Reports (UTR), as designated by the FIU. The Company, through its Compliance Officer, is responsible for ensuring that when an UTR is filed, all supporting documentation and information about why the transactions, as well as the Player, have been flagged as unusual must also be submitted. Any employee and/or Company officer having observed unusual activity from a Customer potentially using the products and/or services of the Company for ML/FT/EP must report such suspicion to the Compliance Officer by not later than 24 hours from when such suspicion is formed. The Compliance Officer, upon receipt of such report, must initiate an investigation into the unusual activity and/or transaction and verify if such suspicion is objectively justified. This is to be done in the shortest time possible. This notwithstanding, the Compliance Officer may continue to investigate to gather the evidence required to submit a complete UTR.

The FATF website is checked regularly to keep abreast with the latest updates and blacklist jurisdictions as well as jurisdictions that do not abide by FATF and other relevant anti-money laundering regulations.

The definition of an unusual transaction and the range of transactions that may be related to money laundering, terrorist financing, or proliferation financing (ML/TF/FP/PF) is broad and not exhaustively defined. Curaçao AML legislation distinguishes between objective and subjective indicators for identifying unusual transactions as defined under the National Decree implementing the NORUT (AB 2017 no. 104, a.a.),

Objective indicators are defined by national decree and must be reported when triggered, regardless of any suspicion.

Subjective indicators are based on the professional judgment of the Company and its employees.

Unusual activity is typically characterized by transactions or behaviors that are inconsistent with the Customer's known transaction patterns, declared economic profile, or expected deposit and wagering behavior. To reasonably determine whether activity is unusual, multiple contextual elements must be considered in combination.

The Company must ensure that it maintains adequate Customer knowledge and monitoring procedures to detect such anomalies in a timely manner and report them as required. Recognizing a transaction or activity as unusual is essential to triggering internal escalation and potential reporting to the FIU.

Any unusual behavior needs to be reported to the FIU. If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of ML/FT/FP, this transaction or series of transactions will be reported to the Public Prosecutor's Office.

Examples of what might constitute unusual transactions/activities related to ML/FT/FP are listed in Annex B of this Policy. The relevant list is not exhaustive, nor does it include all types of transactions or services that may be requested to be used; nevertheless, it can assist the Company and its employees (especially the Compliance Officer and the Company's Management) in recognizing the main methods used for ML/FT/FP. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds for the payments and intended transactions, the nature and economic/business purpose of the underlying transactions requested, and the circumstances surrounding the activities.

6.8.1. Internal reporting and escalation procedure

Where a frontline employee (First Line of Defense), including Customer Support, KYC, or Fraud personnel, identifies a transaction, pattern, or activity that appears unusual or potentially

suspicious, they must submit an Internal Suspicion Report (ISR) to the Compliance Officer within 24 hours of forming such suspicion.

Upon receipt of the ISR, the Compliance Officer shall initiate an internal investigation without delay. This investigation may include, but is not limited to:

- Reviewing the Player's transactional history and behavioral patterns;
- Cross-checking the Customer's profile, documents, and prior risk assessments;
- Analyzing login data and payment instruments used;
- Requesting additional information or documentation from the Customer, such as clarification of the source of funds or source of wealth or supporting documents;
- Contacting the Customer's bank or financial institution, if necessary, to request a reference letter or further validation of account ownership or legitimacy of funds.

If the Compliance Officer determines that the transaction or activity is to be classified as unusual or suspicious under the National Ordinance on the Reporting of Unusual Transactions (NORUT), an Unusual Transaction Report (UTR) shall be submitted without undue delay to the FIU via the goAML platform.

The ISR serves as both the initial notification form and the evaluation document. It is submitted by the First Line of Defense and reviewed by the Compliance Officer, who uses the same report to record investigative steps, internal findings, and the final decision regarding submission to the FIU. This single-report structure ensures accountability, traceability, and operational efficiency. **A standardized template of the ISR is provided in Annex D of this Policy.**

All supporting documentation, internal findings, correspondence, and records of the investigation must be attached to the UTR as part of the submission package.

The Compliance Officer shall ensure that the account in question is flagged for enhanced monitoring or temporarily restricted, if necessary, to prevent further risk while maintaining compliance with anti-tipping-off provisions.

6.8.2. Knowledge

Professional judgment, as a driver to qualitatively assess subjective indicators, is used to ascertain whether there is ML/FT. If for any reason the Compliance Officer, or any other employee of the Company, is aware or owns information that indicates that any of the above activities may have taken place, are taking place, or will be taking place, the Compliance Officer should immediately proceed with filing a report with the FIU.

To identify unusual transactions, the Compliance Officer shall perform the following activities:

- Monitor continuously any changes in the Customer's financial status, business activities, type of transactions, etc.
- Provide adequate training to all staff who will be in contact with any Customer, agents, Customer's transactional information and/or documentation, operational information and/or documentation, and any other information and/or documentation which can lead to knowledge or suspicion being detected.

6.8.3. Compliance Officer's report to the FIU

All Unusual Transaction Reports (UTRs) are submitted through the goAML reporting portal. After the submission of a UTR, the Company may subsequently wish to terminate its relationship with the Customer concerned for de-risking reasons or to keep the account suspended until further notice/information is obtained from the FIU. In such an event, the Company exercises caution, according to the Law, not to alert the Customer concerned that a unusual transaction report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained by the Compliance Officer to avoid any frustration to the investigations being conducted. If no information and/or directions are given by the FIU, it shall be up to the Company to decide on the best course of action, whilst at all times ensuring that no tipping-off takes place.

Furthermore, after the submission of an UTR, the Customer's account and services rendered concerned are placed under the close monitoring of the Compliance Officer and cease to be operative if deemed appropriate to do so without tipping-off or risking tipping-off the reported individual or entity.

6.8.4. Submission of information to the FIU

The Company ensures that in the case of an unusual transaction investigation by the FIU, the Compliance Officer will be able to provide without delay the following information:

- a. the identity of the holders for which the services have been provided.
- b. the identity of the Beneficial Owners.
- c. the identity of the persons authorized to act on behalf of the Beneficial Owners.
- d. data of the volume of funds or level of transactions used for the services being rendered through the Customer's account.
- e. connected accounts, if any.
- f. concerning specific transactions:
 - the origin of the funds
 - the type and amount of the currency involved in the transaction
 - the form in which the funds were placed or withdrawn, for example, cash, cheques, wire transfers
 - the identity of the person that gave the order for the transaction

- the destination of the funds
- the form of instructions and authorization that have been given
- the type and identifying number of any account involved in the transaction
- any other information which is available and deemed to be essential to the investigation

The Compliance Officer shall perform the following activities:

- Receive and investigate information from the Company's employees on unusual transactions that create the belief or suspicion of money laundering. This information is reported in the ISR or any other form that may be deemed appropriate from time to time by the urgency and severity of the situation. The said reports are archived by the Compliance Officer.
- Evaluate and check the information received from the employees of the Company, concerning other available sources of information and the exchanging of information concerning the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained in the report which is submitted to the Compliance Officer is evaluated based on the ISR, being the basis for investigation. Such report is used by the Compliance Officer to record investigative steps, internal findings, and the final decision regarding submission to the FIU.
- If, because of the evaluation described above, the Compliance Officer decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU.
- If because of the evaluation described above, the Compliance Officer decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision and attaches to the initial ISR.
- To act as a first point of contact with the FIU, upon commencement of and during an investigation because of filing a report to the FIU according as indicated above.
- To maintain a registry that includes the reports of unusual transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the Compliance Officer, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.

6.9. AML Compliance Program

Carletta N.V. maintains a comprehensive AML Compliance Program designed to ensure effective oversight, implementation, and continuous improvement of its AML/CFT framework. The program includes structured responsibilities, clear procedures, training, screening, and independent audit, as required under Chapter V.4–V.5 of the CGA AML/CFT Policy.

Component	Description	Reference
Internal Policies, Procedures, and Controls	The Company maintains documented AML/CFT procedures that define workflows, escalation protocols, and segregation of duties. Each process is mapped to internal controls.	Annex A
Compliance Function Structure	The Compliance Officer is responsible for daily AML oversight, policy updates, CRA validation, and escalation of ISR reports. Supporting roles are outlined in control sections.	Section 7 Annex H
Employee Screening Program	All AML-relevant staff are screened pre-employment and every 24 months. Screening includes ID, references, and qualification review. The full employee screening program is provided in Annex G.	Annex G
Employee Training Program	Role-based AML/CFT training is delivered at onboarding, annually, and upon regulatory changes. Content covers legal obligations, internal procedures, and red flags.	Annex E
Independent Audit and Testing	Carletta N.V. engages an independent auditor or external contractor on a competitive basis to test the AML/CFT Program annually. Selection is based on the candidate's expertise, professional certifications, and recognized qualifications in the field of AML/CFT compliance. The audit scope includes CRA/EDD validation, ISR/goAML handling, control testing, and a review of internal training and documentation procedures.	Section 6.11
Examinations by the Curaçao Gaming Authority	When under examination by and upon CGA's requests during the year, Carletta shall provide information or documentation on its AML/CFT/CFP policies and deterrence and detection procedures.	Section 6.12

6.10. Record keeping and monitoring

The Company shall maintain records of the Customer identification documents obtained during the Customer identification and applied due diligence procedures, as well as all necessary records on transactions (both domestic and international) for compliance with information requests from the competent authorities. Such records shall be sufficient to permit the reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to

provide, if necessary, evidence for prosecution of criminal activity.

The documents/data mentioned above shall be kept for at least five (5) years, which is to start running either from the termination of a business relationship or from the date on which an occasional transaction has been executed.

At the instruction of the FIU, the documents/data mentioned above that may be relevant to ongoing investigations shall be kept by the Company for up to ten (10) years or until the FIU confirms that the investigation has been completed and the case has been closed, whichever comes first.

Furthermore, should the firm require the documents for the institution, prosecution or to defend against any claim for which a longer prescriptive period exists, then such records will be kept until the claim is extinguished or such prescriptive period has elapsed.

6.11. Independent audit

Carletta N.V. maintains an independent audit function as part of its AML/CFT Compliance Program in line with Chapter V.5 of the CGA AML/CFT Policy. The purpose of the independent audit is to assess the effectiveness of the Company's AML policies, procedures, controls, and operational execution.

The audit is performed annually or more frequently if required by material changes in operations, regulatory requirements, or internal risk findings. The audit may be conducted by the Internal Auditor or an external, independent contractor selected on a competitive basis. The selection criteria for external providers include:

- Proven expertise in AML/CFT auditing;
- Professional certifications (e.g., CAMS, ICA);
- Relevant jurisdictional or regulatory accreditation;
- Independence from Carletta N.V.'s day-to-day operations.

The audit scope includes, but is not limited to:

- An evaluation of the Carletta's AML/CFT/CFP manuals;
- Customers file review;
- Compliance management;
- Performance of transaction testing;
- Adequacy of employee training and awareness;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;

- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements;
- An assessment of the adequacy of the record retention system; and
- An assessment of the Company's responsiveness to earlier audit findings.

Findings are compiled into an Audit Report, which is submitted to Senior Management with recommendations and corrective actions. Audit results are reviewed and acted upon within pre-determined deadlines. Audit reports are maintained for a minimum of five years and are available to regulators upon request.

6.12. Examination by the Curaçao Gaming Authority (CGA)

In accordance with Chapter V.6 of the CGA AML/CFT/CFP Policy, Carletta shall provide information or documentation on its AML/CFT/CFP policies and deterrence and detection procedures to the examiners of the CGA in preparation of or during an examination and upon CGA's requests during the year.

The following items shall be made readily available:

- The written and approved AML/CFT/CFP compliance program;
- Records of its Business Risk Assessment (BRA);
- The name of each Compliance Officer responsible for Carletta's overall AML/CFT/CFP policies and procedures and his/her designated job description;
- Records of UTRs;
- Records of unusual transactions that required closer investigations;
- Records of frozen accounts;
- Schedule of ML/FT/FP training provided to Carletta's employees;
- The assessment report on Carletta's AML/CFT/CFP policies and procedures by the internal audit department or an external auditor;
- Customers' files, including Customer Risk Assessment, CDD, customer acceptance and transaction information.

7. AML GOVERNANCE & RESPONSIBILITIES

Current legislation enforces Customer Due Diligence on transactions, and having this process in place, has made such activity harder for those intent on laundering money generated from illegal activities. It is of utmost importance to the Company that the policies and procedures are structured in a way that ensures compliance with regulators and legal frameworks, ensuring that the Company is not an attractive vehicle for terrorist financing.

The Company's AML and CTF policies, procedures, and internal controls are designed to ensure compliance with all applicable legislation and best practice procedures. The policies are reviewed and updated regularly to ensure all applicable procedures and internal controls are up to date to account for both changes in regulation and internal changes that could present new risk factors.

The following departments are directly targeted by the requirements of this procedure:

Board of Directors – Approval and Signature requirements, especially in high-risk scenarios, availability of sufficient resources for AML compliance.

All Key Functions – Knowledge of procedure and understanding of requirements.

Customer Support – Understanding of onboarding and reporting requirements.

KYC Department – Understanding and applying DD requirements.

Security – Understanding DD requirements.

Fraud – Understanding the difference between a fraud case and an ML case.

Finance Department – Understanding the risks posed by ML/TF/FP (Refer to Chapter 7).

Legal Department – Ensuring all legislative requirements are met.

Compliance Officer – Refer to the CGA Requirements for Compliance Officer Based on NOIS/NORUT included in **Annex H**.

All Key Functions (including Customer Support, KYC Provider, Antifraud, Finance, and Legal when applicable) collectively form part of the First Line of Defense and are responsible for applying and executing AML/CTF controls within their business operations. The scope of this procedure may be extended to other departments if the need ever arises and all employees need to be attentive and aware of the information flow regarding the prevention of money laundering and funding of terrorism and proliferation of weapons of mass destruction.

The functional responsibilities of departments and personnel involved in AML/CTF implementation are further illustrated in the Company's Three Lines of Defense structure presented in **Annex A** of this Policy.

The Compliance Officer shall belong hierarchically to the management level of the Company's organizational structure to command the necessary authority. Furthermore, the Compliance Officer shall lead the Company's Money Laundering Compliance procedures and processes and report to the Senior Management. The Compliance Officer shall also have access to all relevant information necessary to perform his duties. The level of remuneration of the Compliance Officer shall not compromise his objectivity.

The legally prescribed responsibilities of the Compliance Officer are included in **Annex H - Responsibilities of the Compliance Officer as required by the CGA**. In addition, within the Company it is the Compliance Officer's responsibility:

- To ensure the preparation and maintenance of the lists of Customers categorized following a risk-based approach, which contains, among others, the names of Customers, their account numbers, and the dates of the commencement of the Business Relationship. Moreover, the Compliance Officer ensures the updating of the said list with all new or existing Customers, in the light of any additional information obtained.
- To detect, record, and evaluate, at least on an annual basis, or on the happening of any event which might have an impact on the overall risk, all risks arising from existing and new Customers, new financial instruments and services, and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks should it be required and appropriate to do so.
- To evaluate the systems and procedures applied by a third party with whom the Company has entered into a reliance agreement in terms of Customer Due Diligence including Customer Identification and Verification of the Customer, Identification & Verification of Beneficial Owners as well as the Purpose & Intended Nature of the Business Relationship applied and approves the cooperation with such third parties.
- To ensure that all the branches and subsidiaries of the Company, if any, have taken all necessary measures for achieving full compliance with the provisions of the Anti-Money Laundering Compliance Policy, concerning Customer identification, due diligence, and record-keeping procedures.
- To provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing.
- To acquire the knowledge and skills required for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing.
- To determine whether the Company's departments and employees require further training and education for preventing Money Laundering and Terrorist Financing and organizing appropriate training sessions/seminars. In this respect, the Compliance Officer shall prepare and apply an annual staff training program. Also, the Compliance Officer assesses the adequacy of the education and training provided.
- To prepare the Annual Report, as required by the FIU and any other applicable authority.
- To respond to all requests and queries from the FIU, provide all requested information and fully cooperate with the FIU, if required.
- To maintain a registry that includes the reports of unusual transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the Compliance Officer, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.
- To review the Customer's files and to approve or reject prospective High-Risk Customers.
- To develop and establish the Customer Acceptance Policy and submit it to the Senior Management for consideration and approval.

- To review and update the Anti-Money Laundering Compliance Policy as may be required from time to time, and for such updates to be communicated to the Senior Management for their approval, at least annually or at any such period as may be deemed necessary by the Compliance Officer.
- To monitor and assess the correct and effective implementation of the policy practices, measures, procedures, and controls and in general the implementation of the Anti-Money Laundering Compliance Policy. In this respect, the Compliance Officer shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. If the Compliance Officer identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures, and controls, shall give appropriate guidance for corrective measures and where deemed necessary to inform the Senior Management.

The Financial Department Management and staff are responsible for monitoring all transactions to and from the Company and verifying the identity of all online registered Players requesting a withdrawal, who have reached the XCG 4,000. They must also establish parameters by which any suspicious activity can be immediately noted, and form procedures by which to solve these issues while keeping the risk to a minimum. Such staff must follow the guidelines and requirements as per the Kingdom Sanctions Act, NOIS, NORUT, Sanction National Ordinance, Regulations, EU Directives on the Prevention of Money Laundering and Funding of Terrorism, and any other applicable laws and regulations.

The above-mentioned regulations require obliged entities to verify the Player in such a way that the source of funds is also identified. The verification process will be documented in such a way that every Player will have a risk profile, and file, and, if any Unusual Transaction Report needs to be filed, all evidence in respect of the Player will be on hand.

Carletta N.V. maintains a structured internal control framework aligned with the Three Lines of Defense model (as defined in **Annex A – Three Lines of Defense**). Internal controls are implemented proportionately to customer risk and are designed to ensure effective prevention, detection, escalation, and reporting of ML/TF risks.

Key elements include:

- Clear separation of duties between business units, the Compliance Officer, and the Internal Auditor;
- Four levels of risk-based control applied to customer accounts, based on CRA classification;
- Pre-defined escalation paths for risk events (see Section 6);

- Integration of automated and manual control measures (e.g., transaction limits, device monitoring);
- Oversight from the Compliance Officer and periodic review of control effectiveness.

Roles within the first line of defense, including the KYC Provider and operational teams, are supported by procedures in **Annex A – Three Lines of Defense**.

8. EMPLOYEE TRAINING PROGRAM

The Company shall ensure that training and updates are provided to employees and key people involved in the prevention of AML and fraud within the Company. Such training may be in-house or from third-party providers. All training provided shall be in line with and in proportion to the roles and duties of the individual employee. Training shall be tailored to the tasks and duties of the employee and the Company shall not adopt a one size fits all approach. Training shall be provided regularly and when needed. However, a yearly refresher course shall be provided to ensure that all employees are up to date on recent developments.

Records of such training received shall be kept on file as proof of attendance in such training.

8.1. Employees' obligations

- (a) The Company's employees shall be personally liable for failure to report any information relating to knowledge or suspicion, regarding money laundering or terrorist financing.
- (b) the employees must cooperate and report internally, without delay, and by not later than 24 hours, anything that comes to their attention concerning transactions for which there are grounds for suspicion that the person is involved in money laundering or terrorist financing.
- (c) according to the applicable Law, the Company's employees shall fulfill their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after they comply with point (b) above.

8.2. Employees' Education and Training

- (a) The Compliance Officer shall ensure that the employees are fully aware of their legal obligations according to the applicable Laws, regulations, directives, and implementing procedures by introducing an ongoing employee education and training program.
- (b) The timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can vary depending on the amendments to legal and/or regulatory requirements, employees' duties as well as any other changes in the system of Curaçao.

- (c) the training program aims to educate the Company's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose.
- (d) the training program will have a different structure for new employees, existing employees, and different departments of the Company according to the services that they provide.
- (e) On-going training shall be given at regular intervals to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The Compliance Officer shall ensure that records of the Company's employee training program, including participation and content, are maintained and summarized in internal compliance reporting.

Refer to **Annex 1 – Ongoing Employee Training Program** for more details.

8.3. Compliance Officer Education and Training Program

The Compliance Officer shall be responsible for any updates to the Law and attend any external training necessary. Based on his/her training the Compliance Officer will then provide training to the employees of the Company.

The main purpose of the Compliance Officer training is to ensure that relevant employee(s) become aware of:

- the Law and the Regulations
- the Company's Anti-Money Laundering Policy
- the statutory obligations of the Company to report unusual transactions
- the employee's own personal obligation to refrain from activity that would result in money laundering
- the importance of the Customers' due diligence and identification measures requirements for money laundering prevention purposes.

The Compliance Officer shall document his or her own participation in relevant AML/CFT training and ensure that such information is available to Senior Management and, where applicable, included in compliance reporting and oversight materials.

9. CONSEQUENCE OF NON-COMPLIANCE (NOIS and NORUT)

Under the National Ordinance on the Identification when rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT), failure to comply with AML/CFT obligations may result in significant legal consequences for the Company and its responsible officers.

9.1. Sanctions for Non-Compliance

- Administrative fines imposed by the supervisory authorities;
- Criminal sanctions, including imprisonment, for willful or grossly negligent breaches;
- Revocation of licenses or regulatory permissions issued by the Curaçao Gaming Authority (CGA);
- Public naming and reputational damage via enforcement disclosures.

9.2. Personal Liability of Responsible Officers

Company officers, directors, and senior management may be held personally liable for:

- Failure to implement or enforce adequate AML/CFT procedures;
- Failure to report unusual transactions within the required timeframe;
- Knowingly or negligently ignoring unusual activity of Players;
- Engaging in or facilitating tipping-off.

In accordance with Curaçao law, such breaches may lead to civil, administrative, or criminal penalties, depending on severity and intent.

The Company ensures that all relevant personnel are trained on these obligations and that responsibilities under NOIS/NORUT are clearly defined and documented.

10. AGENTS/INTERMEDIARIES

The Company shall be responsible for creating and maintaining its customer base, and, for the foreseeable future, shall not engage any intermediaries or Agents nor shall it accept Customers coming from such individuals or entities. Should the Company decide to change its policy on the above, a more detailed policy is to be created and approved by the Board of Directors, highlighting how such entities will be handled in line with the applicable legislation and regulation at that time. Introducers, such as affiliates, do not fall within such category as their role is to merely introduce the Customer to the Company and will have no further involvement in the business relationship.

11. RELATED INFORMATION

This Policy should be read in conjunction with:

- CGA AML/CFT Policy (January 2025);
- National Ordinance on the Reporting of Unusual Transactions (NORUT);
- National Ordinance on the Identification when rendering Services (NOIS);
- FATF 40 Recommendations;
- Kingdom Sanctions Act (Rijkssanctiewet);
- goAML Portal & Reporting Guidelines;
- Transparency International Corruption Perceptions Index (CPI);
- **Annex A – Internal Control Structure: Three Lines of Defense**
- **Annex B – Trigger-Based Risk Scoring Table**
- **Annex C – Jurisdiction Risk Classification and Prohibited Countries List**
- **Annex D – Internal Suspicion Report Form (ISR)**
- **Annex E – AML/CFT Training Plan**
- **Annex F – Examples of Unusual Transactions**
- **Annex G – Employee Screening Program**
- **Annex H - Responsibilities of the Compliance Officer as required by the CGA**
- **Annex I – Ongoing employee training program**

12. CONTACT INFORMATION

For questions, compliance support, or to report suspicious activity, please contact:

Compliance Department

Carletta N.V.

Email: finance@pin-up.team

Phone: +447458197085

ANNEX A - Internal Control Structure: Three Lines of Defense

This diagram below illustrates the Company's Three Lines of Defense model, which defines the allocation of roles and responsibilities in the prevention of money laundering, terrorist financing, and proliferation of weapons of mass destruction and other financial crimes.



First Line of Defense – Operational Functions

The first line of defense is composed of all operational departments and service providers directly involved in Customer interaction and transaction processing. This includes the KYC/Onboarding Provider, Customer Support, Fraud and Security Team, and the Finance Department. These units are responsible for applying due diligence measures, performing ongoing monitoring, and detecting potentially unusual or suspicious activity during day-to-day operations.

Second Line of Defense – Compliance Oversight

The Compliance Department acts as the second line of defense by providing independent oversight, developing and maintaining the AML/CFT framework, and reviewing alerts or escalations from the first line. The Compliance Officer and Investigation Unit (usually lawyer's team) assess whether activities or transactions meet the threshold for reporting to the FIU and ensure the ongoing adequacy of AML controls.

Third Line of Defense – Internal Audit

The third line of defense provides independent assurance of the effectiveness of the Company's AML/CFT Policy. The Internal Auditor evaluates the design and operational effectiveness of the controls implemented by the first and second lines, and reports findings to Senior Management and the Governing Body.

Oversight from the Governing Body / Audit Committee and Senior Management, including the CEO, ensures strategic supervision, resource allocation, and accountability. The Company also remains subject to independent evaluation by External Audit and regulatory supervision by the Regulator.

ANNEX B - Trigger-Based Risk Scoring Table

The table below includes a detailed list of risk triggers categorized by type, along with example behaviors and the associated numerical score used within the Company's AML risk scoring model. These triggers support dynamic risk reassessment and guide the application of due diligence measures.

The trigger-based scoring model used in the CRA derives directly from the Company's Business Risk Assessment (BRA). Each operational trigger listed in Annex B is based on a risk factor that was prioritized in the BRA based on its likelihood and impact.

These prioritized risks are translated into Customer-facing triggers (e.g., structuring, use of VPN, forged ID) and assigned normalized scores (1–3) depending on their relevance and severity. Each such trigger contributes to the Customer Risk Score, supports dynamic reassessment, and may initiate Enhanced Due Diligence (EDD) or an Unusual Transaction Report (UTR) where warranted.

Risk Category	Trigger Description	Example Behavior / Detection	Risk Score
Customer	Multiple accounts from same device	Same device ID used across 2+ user accounts	2
Customer	Refusal to provide SoF	Customer declines to submit source of funds documentation when required during withdrawal or EDD	3
Customer	Unverified or forged documents	Submitted ID has visual anomalies or fails document integrity check	3
Customer	False occupation or inconsistent profile	Declared profession (e.g. student) does not match transaction volume	2
Geographic	Use of VPN or proxy	Login IP address linked to VPN service or shows rapid country switching	2

Risk Category	Trigger Description	Example Behavior / Detection	Risk Score
Geographic	Access from high-risk country	Login or deposit from jurisdiction on FATF blacklist or grey list	3
Geographic	Geolocation mismatch	Deposit from one country, access from another (e.g., card: DE, IP: RU)	3
Product	Fast withdrawal without gameplay	Deposit followed by immediate withdrawal request without wagering	2
Product	Bonus abuse pattern	Multiple bonuses claimed in short period with minimal qualifying activity	2
Product	High-value single game payout	Unusually large win in low-variance game immediately followed by withdrawal	2
Delivery	Third-party payment method	Cardholder name differs from account holder	1
Delivery	Unregulated or anonymous PSP	Deposit via crypto/PSP without license or transparent ownership	3
Delivery	Frequent changes in payment method	User adds/removes 3+ payment methods within 7 days	3
Behavior	Structuring	Multiple small deposits (e.g., XCG 3,900) just below threshold to avoid SoF trigger	3
Behavior	Churning activity	Frequent deposits and withdrawals with limited or no gameplay	3
Behavior	High-frequency failed deposits	User initiates 5+ failed deposits within 24 hours	2

Risk Category	Trigger Description	Example Behavior / Detection	Risk Score
Behavior	Rapid turnover post-KYC	Account dormant, then sudden surge in activity right after ID approval	2
Behavior	Withdrawals to new methods	User changes payment method immediately before withdrawal request	3

ANNEX C - Jurisdiction Risk Classification and Prohibited Countries List

This annex outlines the Company's framework for classifying jurisdictions according to geographical risk. This classification supports onboarding decisions, ongoing customer due diligence (CDD), and monitoring, in line with a risk-based approach under Curaçao AML/CFT regulations.

Countries are grouped into four categories based on regulatory prohibitions, international AML/CFT evaluations, and governance risk indicators.

1. Prohibited Jurisdictions

These are jurisdictions from which the Company will not accept Customer traffic or registrations under any circumstances. Players attempting to register from these jurisdictions must be automatically blocked. Access must be technically restricted and actively monitored.

This includes:

- Countries subject to comprehensive international sanctions or embargoes.

Please follow these links for the most updated lists:

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

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

- Other countries prohibited as per Company policy.

List of other jurisdictions prohibited as per Company policy

Australia. France and its territories. Hong Kong. Italy. Netherlands and its territories (Curacao, Aruba, Bonaire, Saba, Sint Maarten, St. Eustatius).	Singapore. Spain. United Kingdom of Great Britain and Northern Ireland. United States of America.
---	--

Depending on global developments, this list may change from time to time.

2. High-Risk Jurisdictions

These jurisdictions (excluding already prohibited countries) may be accepted only with enhanced due diligence (EDD) and require explicit approval by the Compliance Officer. This group includes:

- Countries listed by the Financial Action Task Force (FATF) as:
 - High-Risk Jurisdictions Subject to a Call for Action, and
 - Jurisdictions Under Increased Monitoring.

Please follow the link to the most updated FATF-lists:

<https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>

- CFATF Public Statements

Please follow the link to the CFATF Public Statements:

<https://www.cfatf-gafic.org/home/public-statements>

- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State annual International Narcotics Control Strategy Report (INCSR)

Please follow the link to the International Narcotics Control Strategy Reports:

<https://www.state.gov/international-narcotics-control-strategy-reports/>

- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime

Please follow the link to the EU list of high-risk third countries:

https://eur-lex.europa.eu/eli/reg_del/2016/1675

- Countries identified by OFAC as presenting elevated financial crime or sanctions risk.

Please follow the link to the most updated OFAC-lists:

<https://sanctionslist.ofac.treas.gov/Home/SdnList>

- Jurisdictions, demonstrating higher exposure to corruption, weak institutions, or political instability, based primarily on the Transparency International Corruption Perceptions Index (CPI). A CPI-range of 0-40 is considered high risk.

Please follow the link to the most recent CPI:

<https://www.transparency.org/en/cpi/2024>

3. Medium-Risk Jurisdictions

Jurisdictions not under sanctions but demonstrating higher exposure to corruption, weak institutions, or political instability, based primarily on the Transparency International Corruption Perceptions Index (CPI). A CPI-range of 41-70 is considered medium risk. EDD may be applied at the discretion of the Compliance Officer.

Please follow the link to the most recent CPI:

<https://www.transparency.org/en/cpi/2024>

4. Standard-Risk Jurisdictions

All jurisdictions not included in the above categories fall under standard risk. Customers from these countries are subject to regular CDD and monitoring unless elevated risks are identified during the Customer risk assessment.

Important Notes

- This classification supports but does not replace individual Customer risk assessments.
- This annex must be reviewed at least annually, and updated when international risk assessments or CGA/ FIU notifications change.
- Customers from high- or medium-risk jurisdictions may still be rejected if other risk factors apply.

Clarification on UNSC Sanctions

The United Nations Security Council (UNSC) Consolidated Sanctions List contains individuals, entities, and groups subject to international sanctions.

It is not a country-level risk classification tool and is therefore not included in this annex. However, screening against the UNSC list is mandatory for all Customers and is handled separately as part of the Sanctions List Screening procedure described in the main AML Compliance Policy.

ANNEX D - Standardized template of the Internal Suspicion Report (ISR)

This establishes the form of report that the Employee must fill in and forward to the Compliance Officer in cases specified in Anti-Money Laundering Compliance Policy. The Compliance Officer must accept the report, and the documents attached to it and consider the need to send a notification to the competent authority or, if necessary, perform other activities.

1. Employee Information • Name of employee submitting the report: • Department / Role: • Date and time of report submission:	
2. Customer Information • Full name of the customer: • Date of birth / National ID or player account number: • Customer jurisdiction (residency or activity location):	
3. Transaction or Behavior Description • Date and time of transaction or behavior: • Amount involved (if applicable): • Description of transaction or unusual activity:	
4. Grounds for Suspicion • Description of trigger or reason for concern: (e.g., structuring, unusual deposit pattern, forged document, excessive withdrawals, etc.) • Type of risk identified: ☐ Money Laundering ☐ Terrorist Financing ☐ Other (please specify): _____	

5. Supporting Documents Attached • ☐ Transaction records • ☐ Chat/email transcripts • ☐ ID documents • ☐ Payment method records • ☐ Other (describe): _____	
6. Compliance Officer Review Section (to be completed by the Compliance Officer) • Date of internal report received: • Actions taken (e.g., transaction analysis, pattern review, SoF/SoW checks, request to bank): • Outcome of internal investigation: ☐ No further action ☐ Ongoing monitoring ☐ UTR submitted via goAML • Date of UTR submission (if applicable): • Reference number of goAML submission: • Notes:	

ANNEX E - Annual AML/CFT Training Plan

This annex outlines the structured training framework adopted by Carletta N.V. for AML/CFT compliance, in accordance with Curaçao AML/CFT Regulations, the Sanctions National Ordinance, and CGA regulatory expectations. The training program ensures that all relevant staff are aware of their obligations under the AML/CFT regime, and are equipped to detect, assess, and escalate ML/TF/FP risks.

1. Objective

To ensure that all employees, contractors, and relevant third-party service providers receive tailored, role-specific training on AML/CFT compliance. Training supports effective implementation of the Company's internal controls, Customer Acceptance Policy (CAP), and goAML reporting obligations.

2. Training Audience and Frequency

- Compliance Officer – Annual, and following material regulatory changes
- Senior Management – Annual
- KYC Provider (KYCAID LIMITED) – Annual
- Customer Support and Payment Staff – Bi-Annual
- Fraud, Risk, and Monitoring Teams – Quarterly
- New Employees – Upon hiring

3. Training Topics

- Curaçao AML/CFT legal framework (NOIS, NORUT, CGA regulations)
- Identifying and reporting unusual transactions
- Using the Internal Suspicion Reporting (ISR) Form
- Escalation process: from detection to goAML reporting
- Sanctions screening procedures and PEP handling
- Customer Risk Assessment (CRA) methodology and red flags
- Practical case studies and simulation of UTR submission

4. Delivery Methods

Training shall be delivered using a blended approach:

- Online modules and case-based quizzes
- Live webinars and instructor-led sessions

- Periodic knowledge assessments
- Internal memos and policy update briefings

5. Records and Evaluation

Attendance logs, completion certificates, and training results will be maintained by the Compliance Officer. Effectiveness of training will be reviewed annually and adjustments made to address evolving risks.

ANNEX F - Examples of unusual transactions/activities related to money laundering and terrorist financing

Money laundering

Under the laws of multiple jurisdictions, money laundering is a serious offense. Money laundering involves various acts committed to conceal or convert property or the proceeds derived from such property (such as money) knowing or believing that these were derived from the commission of a designated offense. In this context, a designated offense means an offense under the Criminal Code (Title XXXI of the Penal Code of Curaçao) or any other applicable law or the equivalent law in the jurisdiction within which such offense has or is suspected to have taken place. It includes but is not limited to those offenses relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion, and copyright infringement amongst others.

Unusual transactions are financial transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offense. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a money laundering offense.

“Reasonable grounds to suspect” is determined by what is reasonable in your circumstances, including normal business practices and systems within the industry. While NORUT and Regulations do not specifically require the Company to implement or use an automated system for detecting unusual transactions, we do have such a system in place.

In this context, “transactions” include both completed and attempted transactions, as previously defined. The Company’s compliance framework incorporates a continuous risk assessment process aimed at identifying potential money laundering or terrorist financing threats. In higher-risk situations, the Company applies enhanced ongoing monitoring measures to ensure that suspicious behavior or patterns are promptly detected, investigated, and, where appropriate, reported to the FIU.

Completed transactions

A completed transaction refers to any financial transaction that has been successfully executed by or on behalf of the Customer. This includes, for example, deposit, wagering, and withdrawal transactions. Even if the Customer requests a withdrawal of unspent funds, such an action is still considered a completed transaction and may fall within the scope of AML monitoring procedures if it appears inconsistent with the Customer’s known profile or expected behavior.

Attempted transactions

An attempted transaction is one that a Customer intended to conduct and took some form of action to do so. An attempted transaction is different from a simple request for information, such as an inquiry as to the fee applicable to a certain transaction. An attempted transaction includes entering negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the Customer. A formal request by the Customer to withdraw funds from their account would constitute such an attempt.

The following are examples of attempted transactions:

- A financial entity or casino refuses to accept a deposit because the Customer refuses to provide identification as requested.
- A securities dealer or life insurance agent refuses to process a transaction - for which the Customer insists on using cash - because their business practice is not to accept cash.
- A Customer of a real estate agent starts to make an offer on the purchase of a house with a large deposit but will not finalize the offer once asked to provide identification.
- An individual asks an accountant to facilitate a financial transaction involving large amounts of cash. The accountant declines to conduct the transaction.
- A money services business will not process a request to transfer a large amount of funds because the Customer requesting the transfer refuses to provide the identification requested.

To report an attempted transaction, it must be one that you have reasonable grounds to suspect that it is related to money laundering or terrorist financing. An attempt to conduct a transaction does not necessarily mean the transaction is suspicious/unusual. However, the circumstances surrounding it might contribute to your having reasonable grounds for suspicion.

Transactions related to terrorist property

In line with Curaçao AML/CFT Regulations and the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company monitors for activity that may indicate attempted or completed transactions involving terrorist property or the financing of terrorism. While such transactions may not always be clearly labeled as terrorist-related, the following patterns may give rise to suspicion and warrant immediate escalation to the Compliance Officer. The following are examples of red flags that may indicate such risks. This list is non-exhaustive, and other circumstances may also be deemed by the Company to constitute transactions related to terrorist property or terrorist financing, based on the context, available information, and risk assessment:

1. Unusual use of foreign or high-risk payment instruments: use of prepaid, business, or third-party cards not consistent with the Player's declared profile or country; use of payment

methods originating from or linked to jurisdictions known for terrorist financing risks or FATF high-risk classification.

2. Anonymity and account layering behavior: frequent switching of devices or accounts with overlapping attributes (e.g., same IP, same device ID); multiple accounts linked to similar addresses, payment methods, or devices—indicating possible use of mules or proxies.
3. Suspicious deposit and withdrawal behavior: large deposits made with no gameplay or minimal turnover, followed by withdrawal requests; structuring of transactions to avoid detection (e.g., multiple deposits just under risk threshold); attempt to withdraw funds to newly added payment methods or accounts not previously verified. No meaningful gaming activity between deposit and withdrawal (pure money movement).
4. Geographic and identity inconsistencies: accounts accessed from or funded via countries with elevated TF risks, using VPNs or proxies; discrepancies between declared personal details and the geographic origin of funds or access points.
5. Behavior that indicates possible channeling of funds: use of gaming accounts solely for deposit and withdrawal cycles without genuine gaming activity; repeated cancellation of bets or unusual in/out flows inconsistent with the Customer's risk profile.
6. Use of high-risk payment providers: use of lesser-known, offshore, or unlicensed PSPs (Payment Service Providers), especially those operating without clear KYC obligations; known facilitation of anonymous funding (e.g., crypto-fiat mixers, cash-funded prepaid vouchers).
7. Unusual behavior such as the cancellation of a withdrawal shortly after submission, particularly following account verification or bonus fulfillment, may warrant further investigation.
8. A Player is unwilling to provide sufficient or accurate information during onboarding or enhanced due diligence, including the purpose of using the gaming account, expected transaction behavior, or the source of funds and source of wealth. The information submitted may appear minimal, vague, or unverifiable, raising concerns regarding the legitimacy or transparency of the Player's profile.
9. A Player provides identification documents that raise concerns due to poor quality, inconsistencies, or lack of verifiability, which may indicate an attempt to conceal true identity or avoid proper due diligence.
10. A Player fails to provide required verification documents in a timely manner, or repeatedly submits incomplete or inconsistent documentation, potentially indicating an attempt to avoid proper due diligence.
11. Unexplained inconsistencies arising during the process of identifying and verifying the Customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address, and date of birth, etc.).

ANNEX G - Employee screening program

All employees and contractors assigned to AML/CFT-relevant roles must undergo a documented screening process before being granted access to AML-related functions.

Scope of Screening

- Identity verification (government-issued ID);
- Employment reference checks;
- Verification of qualifications relevant to the role;
- Screening against internal watchlists and external sanctions lists;
- Confirmation of clean disciplinary and criminal background (where allowed by law).

Ongoing Screening

- Re-screening occurs at least once every 24 months;
- Additional screening is required upon promotion, transfer to sensitive roles, or performance-related incidents.

Screening outcomes are documented and maintained by the Compliance Department and may be shared with management upon request.

ANNEX H - Responsibilities of the Compliance Officer as required by the CGA⁴

5. Scope of Responsibilities

The operator must formally designate a senior officer at the management level as responsible for detecting and deterring money laundering and terrorist financing. This AML/CFT Compliance Officer should have timely access to customer identification data, Customer Due Diligence (CDD) information, transaction records, and other relevant data, and must be able to act independently.

The Compliance Officer is responsible for:

- Designing and implementing the AML program.
- Ensuring compliance with Curaçao laws and regulations regarding money laundering and terrorist financing.
- Reviewing adherence to the casino's policies and procedures.
- Organizing staff training sessions on compliance-related issues.
- Analyzing transactions and identifying those subject to reporting under the Ministerial Decree on Indicators for Unusual Transactions.
- Reviewing internally reported unusual transactions for completeness and accuracy.
- Maintaining records of both internally and externally reported unusual transactions.
- Design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts
- Conducting further investigations into unusual transactions if necessary.
- Preparing external reports on unusual transactions.
- Making necessary changes to the AML program.
- Staying informed about local and international developments related to money laundering and terrorist financing and suggesting improvements to management.
- Preparing periodic reports on the casino's efforts against money laundering, terrorism financing, and proliferation financing.

⁴ GCB Requirements for Compliance Officer Based on NOIS/NORUT, implementation date January 1, 2025.

ANNEX I – Ongoing employee training program

In compliance with Chapter V.4 of the CGA AML/CFT Policy, the Company shall develop training programs and provide training to all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree Indicators Unusual Transactions (N.G. 2015 no. 73, as amended). Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the casino's policies against money laundering and terrorist financing. Most areas of the Company shall receive training and the target audience shall include most employees. Each segment shall be trained on topics and issues that are relevant to them.

Training must at least address the following topics:

a. New employees

- The nature and process of ML/FT/FP, specifically methods and trends in the Company's specific business line.
- The need to report any unusual transactions to the appropriate designated officer. Shall be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority.
- The existing internal policies, procedures and regulations concerning ML/FT/FP and the reporting requirements.
- CDD
- Objective and subjective indicators for UTRs.

b. Employees tasked with the first line of defense against ML/FT/FP

- The importance of AML/CFT/CFP, including some basics.
- ML/FT/FP typologies using online gaming companies.
- The Company's procedures to equip them to recognize potential ML/FT/FP and the actions to take.
- Personnel involved with account opening shall be made aware of the need to verify the identity of the customer.

c. Audit staff

These are employees charged with overseeing, monitoring and testing money laundering controls.

- Changes in regulation, money laundering methods and enforcement, and their impact on the organization.

d. AML/CFT/CFP Compliance staff

These are employees who run the AML program.

- Specialized training to stay on top of new trends or changes that impact the Company and the way it manages risk. This will require attending conferences or AML/CFT/CFP-specific presentations to go into greater detail.

e. Supervisors and Managers

Those tasked with the responsibility to supervise or manage the staff.

- A higher level of instruction covering all aspects of ML/FT/FP, procedures and regulations

f. Senior management and board of directors

Money laundering issues and dangers should be regularly and thoroughly communicated to Senior Management and Board to keep them aware of the reputational risk that money laundering poses to the Company.

Refreshment training

Refreshment training shall be arranged at regular intervals to ensure that employees are kept informed of current and new developments regarding ML/FT/FP techniques, methods and trends.

Record keeping

To demonstrate compliance with employee training guidelines, the Company shall maintain records that include:

- Details on the content of the training programs;
- The names of the employees who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure employee understanding of ML/FT/FP requirements; and
- An ongoing training plan.