

Mr. Cedric Pietersz
Curaçao Gaming Authority
Scharlooweg 172-174
Willemstad-Curaçao

30 May 2025

Re: Uploading AML/CFT Policy

Dear Mr. Pietersz,

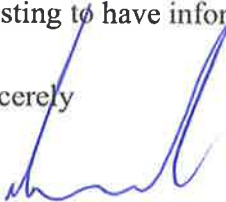
In order to comply with the due date for submission of the AML/CFT Policy, the applicant hereby uploads the draft version of the AML/CFT policy.

Note that this policy is not yet final as it is under review by management for approval and sign off.

Once approved, the final and official version will be signed off by management and uploaded to the portal. We expect this to take place in the course of the coming week.

Trusting to have informed you accordingly.

Sincerely



Raoul Behr
Managing Director

Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) Policy (Curacao)

Document information			
Document name:	PowerPlay - AML & ATF Policy (Curacao)		
Document version:	1.3	Date of approval:	26.05.2024
Approved by:	CEO	Revision interval:	At least annually
Document owner:	Compliance Director	Information classification:	Internal
Market	Curacao		
Revision history			
Author:	Version:	Date:	Change history:

Head of Compliance	1.0	24.02.2020	Initial release
Head of Compliance	1.1	16.03.2020	Approved version
Head of Compliance	1.1	15.03.2021, 15.03.2022, 15.03.2023	Annual review
Head of Compliance	1.2	02.08.2024	Proposed change before 01.09 AM update
Compliance Director	1.3	26.05.2025	System change update
Compliance	1.4	30.05.2025	General update

Contents

1. General	
1.1. Introduction	
1.2. List of relevant documentation	
1.3. Definition	
1.3.3. <i>Similarities and Differences of ML & TF</i>	
2. Legislation and Guidelines	
2.1. Relevant Legislation	
2.2. Curaçao Gaming Authority Guidelines	
2.3. Financial Action Task Force (FATF) 40 Recommendations	
3. Responsibilities	
3.1. Senior Management	
3.2. Verification Department	

3.3. Compliance Officer	
3.4. Company's Employee's Responsibilities	
4. Customer acceptance	
4.1. Player Identification - Know Your Client ("KYC")	
4.2. Politically Exposed Person ("PEP")	
4.3. Sanctions Screening	
5. Customer relationship	
5.1. Structure of the customer relationship	
5.2. Identification & verification	
5.2.1. <i>Player risk assessment</i>	
5.2.2. <i>Simplified Due Diligence</i>	
5.2.3. <i>Enhanced Due Diligence</i>	
5.2.4 <i>Reliance on third parties to perform customer due diligence</i>	
5.3. Ongoing Monitoring	
5.4. Unusual transactions	
5.5. Termination of a business relationship	
5.6. Documentation of Due Diligence	
6. Risk-Based Approach	
6.1. Objectives	
7. Regulatory Reporting	
7.1. Internal Reporting Procedures	
7.2. Reporting to the FIU	
7.3. Confidentiality	
8. Protection of employees and whistleblowing	
9. Training	
10. Record keeping	
10.1. Types of Documents to be Retained	
10.2. Storage of Records	
10.3. Retention Period	
10.4. Secure Disposal of Records	
10.5. Monitoring and Review	
10.6. Employee Training on Data Retention	

1. General

1.1. Introduction

Deck Entertainment B.V. ("Company", "Deck", "We") is a remote gambling operator offering casino and sportsbook services and have B2C online gambling license granted on April 3, 2025, by Curaçao Gaming Authority ("CGA"), license number OGL/2024/999/0482.

The Company is obliged to respect rules indicated in Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction.

The gaming industry operating in and from Curaçao is held to compliance with, among other, the National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID)), and the National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT)).

With the publication of the National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverleningkansspelsector) and the National Decree supervisorunusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector), the Curaçao Gaming Authority (CGA) is tasked with the AML/CFT supervision of the gaming sector operating in and from Curaçao.

Curacao's financial intelligence unit is Financial Intelligence Unit Curacao ("FIU Curacao").

For a comprehensive overview of the applicable legal framework, see section 2.1. below.

The objectives of this policy are, amongst others:

- ensuring Company's compliance with all applicable laws, statutory instruments of regulation, and requirements of the relevant supervisory body;
- protecting the Company and all its staff as individuals from risks associated with breaches of laws, regulations and supervisory requirements;
- preserving the good name of Company against the risk of reputational damage presented by implication of money laundering and terrorist financing activities;
- making a positive contribution to the fight against crime and terrorism.

To achieve these objectives, **it is our policy to ensure** that:

- every staff member shall meet their personal obligations as appropriate to their role and position within the Company;
- commercial considerations shall never be permitted to take precedence over the Company's AML & ATF commitments;

Any failure to follow this Policy (and its associated Compliance Procedures) could severely harm Deck's reputation, financial standing and possibly breach the terms of the licenses and registrations necessary to operate our businesses. Such a failure may result in disciplinary action or termination for any employee found to have breached this Policy and may constitute a criminal offence. It should also be remembered that our compliance obligations include all our Policies and Procedures as well as those requirements that arise from the numerous contractual relationships with card schemes, banks and other payment related partners that we have entered into business relationship with.

This policy applies to all employees, contractors, directors and any other individuals or entities acting on behalf of the Company, including those involved in customer interaction, transaction processing, compliance, risk management and account oversight. It is also relevant to third-party service providers, partners, and agents who perform functions on behalf of the Company where there is a risk of exposure to money laundering or terrorist financing activities.

For any questions regarding this policy, please feel free to contact the Compliance Director; Edyta Miaskiewicz via email compliance@powerplay.com.

1.2. List of relevant documentation

The whole Company AML program consist of this Policy and AML relevant documentationsuch as:

- 1.2.1. Know Your Client Procedure
- 1.2.2. Player Account and Fund Management Policy
- 1.2.3. Account Closure, Reopen and Suspension Procedure
- 1.2.4. Internal Reporting Policy
- 1.2.5. External Reporting Policy
- 1.2.6. Player Risk Management Policy

1.3. Definition

We believe that prior to implementing the AML&ATF Policy, it is essential for it to identify what is, on the one hand, money laundering, and what, on the other hand, constitutes financing of terrorism.

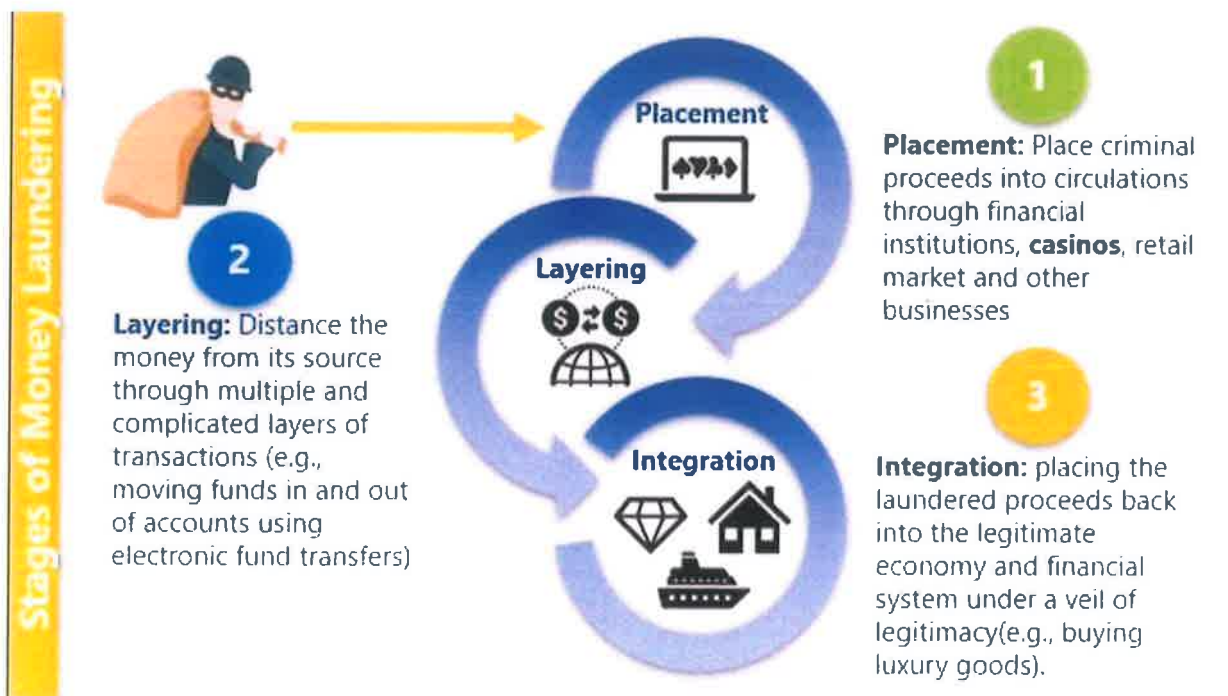
1.3.1. Money Laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. Essentially, money laundering is the process whereby “dirty money”

– produced through criminal activity – is transformed into “clean money”, the criminal origin of which is difficult to trace. Profit-motivated crimes span a variety of illegal activities from drug/weapon/human trafficking and smuggling to fraud, extortion and corruption.

Money laundering facilitates corruption and can destabilize the economies of susceptible countries. It also compromises the integrity of legitimate financial systems and institutions and gives organized crime the funds it needs to conduct further criminal activities. It is a global problem, and there are numerous different techniques that can be very sophisticated. Technological advances provide further opportunities to launder illegal profit and obscure the money trail leading back to the underlying crime.

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process: Placement, Layering and Integration.



1.3.2. Terrorist Financing

Terrorist financing provides funds for terrorist activity which has as its main objective to intimidate a population or compel a government to do something. This is done by seriously interfering with or causing damage to essential services, facilities, or systems, or by endangering, harming or killing people.

Terrorist financing may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

To move their funds, terrorists use the formal banking system, informal value-transfer systems, Hawalas and Hundis and, the oldest method of asset-transfer, the physical transportation of cash, gold and other valuables through smuggling routes.

The funding flow usually follows a linear pattern: collection of funds, storage of funds, movement of funds, usage of funds.



Financing of Proliferation of Weapons

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

1.3.3. Similarities and Differences of ML & TF

1.3.3.1. Similarities

Money laundering and terrorist financing offences can be committed in connection with each other. For example, the funds for terrorist activity can be 'laundered' funds.

1.3.3.2. Differences

While they may share similar typologies, the difference lies in the timing and direction of the flow of funds and transactions.

Criteria	Money Laundering	Terrorist Financing
Motivation	Profit making	Ideological purposes
Intention	Disguise the origin of the resources	Intimidate through violence
Source of Financing	Illegal Resources Extortion Kidnapping Drug-trafficking Smuggling Fraud Theft	Illegal Resources Extortion Kidnapping Drug-trafficking Smuggling Fraud Theft Legal Resources Donations Government sponsorship Controlled companies
Methods	Placement Layering Integration	Placement Layering Integration
Life Cycle	Circular	Linear

1.4 The risk-based approach

Deck Entertainment B.V. adopts a risk-based approach in our AML/CFT/CFP compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF/PF risks specific to the online gaming industry. When developing its AML compliance program, we assessed risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Deck Entertainment B.V. may employ simplified measures.

To effectively apply the risk-based approach, Deck Entertainment B.V. conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

Deck Entertainment B.V. shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. Deck Entertainment B.V. shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

1.5 Business Risk Assessment

The Business Risk Assessment (BRA) framework is a crucial component of Deck Entertainment's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

Deck Entertainment B.V. performs BRAs thoroughly evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

2 Legislation and Guidelines

2.3 Relevant Legislation

This section outlines the key legislative and regulatory frameworks that govern Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Countering the Financing of Proliferation (CFP) in Curaçao. It is essential for ensuring compliance with local and international standards, particularly for businesses operating in the gambling sector.

With view of promoting compliance with the laws and decrees with regard to AML, CTF and CFP, and to implement sound internal policies and procedures to combat money laundering and the financing of terrorism, the following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282)
- National Decree supervisor unusual transactions gaming sector (L.B, 28.01.2019, no. 19/0283)
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Decree prohibition of import, export, and transit of Venezuelan Gold (N.G. 2019, no. 82).
- National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no.74) as amended by (N.G. 2014, no. 90).

The Company regularly reviews and updates their policies and procedures to reflect any changes in local laws and regulations, ensuring ongoing adherence to the latest legal requirements and guidelines.

2.4 Curaçao Gaming Authority Guidelines

For the purposes of supplementing and providing additional elaboration to the local regulatory landscape, the Curaçao Gaming Authority has published The Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction, which are an integral part of the land-based and the online gambling licenserequirements for the Curaçao jurisdiction, effective as of 15.05.2024.

2.5 Financial Action Task Force (FATF) 40 Recommendations

The Financial Action Task Force (FATF), established by the G-7 Summit in 1989, sets global standards for combating money laundering and terrorist financing. The Dutch Kingdom is a member of FATF, and Curaçao is part of the Caribbean Financial Action Task Force (CFATF). The FATF's 40 Recommendations are integrated into local laws by member countries to ensure effective control of financial crime. The Company shall ensure compliance with the FATF Recommendations, particularly the sector-specific recommendations and those pertaining to Customer Due Diligence.

3 Responsibilities

3.3 Senior Management

For the AML & ATF purposes the Senior Management in the Company are Company Directors.

Senior Management is fully engaged in the process around the Company's assessment of risks for money laundering and terrorist financing and is involved in the process of decision making, to develop the appropriate policies and processes to comply with relevant legislation.

Senior Management fully supports the Compliance Team and ensures appropriate standards are implemented within their field of interest, for example by clear communication of applicable procedures to their staff members. Further, they will ensure robust mechanisms are in place to make sure that all policies and procedures are carried out effectively, weaknesses are identified, and improvements are made where necessary. Senior Management is responsible for regular reporting to the Board about AML/CFT company state at least annually.

3.4 Verification Department

The Verification Department is responsible for conducting customer due diligence checks (standard and enhanced) and applying any required measures in line with the implemented approach. This Department is also responsible for ongoing customer monitoring of all related transactions and applying any measures that are necessary.

Furthermore, the Company has established, implemented and is continuously monitoring the compliance with comprehensive procedures for relevant staff to adhere to in case of anomalies and/or red flags identified in the course of the customer due diligence (CDD) process.

The company has developed internal systems, procedures and controls suitable for the remote gaming environment and provided the team with appropriate tools and training to perform the required checks.

3.5 Compliance Officer

The Company has appointed a Compliance Officer ("CO"). The CO is responsible for ensuring that the company complies with all relevant anti-money laundering (AML), counter financing of terrorism (CFT), and counter financing of proliferation (CFP) regulations. The CO's duties include developing and maintaining the company's AML/CFT/CFP policies and procedures, conducting risk assessments, and overseeing the implementation of compliance measures. The CO must stay informed about changes in relevant laws and regulations and ensure that the company adapts its practices accordingly.

The Company ensures that the individual appointed as the CO enjoys sufficient authority and command to be able to act independently of its management. The CO shall have access to all necessary information/documentation and company employees to effectively carry out their obligations. The CO maintains direct lines of communication with senior management to ensure accountability and transparency. Regular reports on the status of the AML/CFT/CFP program, including any identified risks, compliance issues, and corrective actions, are provided to the Board of Directors and the CEO

3.6 Company's Employee's Responsibilities

All staff communicating with the customers, or having access to information about clients' affairs, receive anti-money laundering training. In this manner, they are able to identify which player's

actions should reasonably lead them to suspect money laundering or terrorism financing risk. The Company undertakes to regularly perform effectiveness assessments of its training programs that staff attends for the purposes of ensuring adequacy of the contents of the trainings and their relevance to the particular role of the staff being trained.

Staff is expected to recognize and understand any gaming or transaction behavior which might indicate the customer being involved in money laundering or terrorism financing.

Where they know, suspect or have reasonable grounds to know or suspect that they are dealing with the proceeds of crime, that person must submit an internal report to the CO, according to the Reporting Procedure. In this manner, the employee's legal obligation to report will be considered to have been fulfilled. Employees are also made aware that, if they do not make an internal report to the MLRO when necessary, they may also face criminal sanctions.

4 Customer acceptance

The Company shall only accept customers who intend to use our website according to its purpose. Individuals with different intentions or ulterior motives shall not be accepted by the Company. Every customer must register their account personally, the Company does not accept customers registering an account for 3rd parties. The Company will terminate the business relationship if there is a reason to believe that a customer's account is being used by or on behalf of another person. This includes any customers operating an account funded by an Organized Crime Group.

Anonymous accounts are prohibited.

4.3 Player Identification - Know Your Client ("KYC")

The company accepts only players who will successfully fill registration page with:

- Name

- Surname
- Gender
- Date of Birth
- Phone Number
- Permanent Address

Data entered at the registration form shall be automatically checked by AgeChecked software against independent data to verify the player's identity. Additionally, PEPs and Sanction check also shall happen at this stage. Depending on the outcome, player can be verified and allowed to deposit and play or shall be sent for further manual verification.

Manual verification is being made in the GiG software system where whole process can be tracked and documented.

Every player is also asked to upload additional documentation (if needed) before first withdrawal is processed. Only identified and successfully verified player are able to withdraw their balance.

More information about the process can be found in the Know Your Client (KYC) Policy.

4.4 Politically Exposed Person ("PEP")

A PEP is an individual who is or has been entrusted with a prominent public function, such as serving in a prescribed government office or a political position, which can make them vulnerable to corruption and potential target of criminals who could exploit their status and use them knowingly or unknowingly to carry out ML/TF activities.

At the moment of registration, the Company is gathering attestation from players whether they are a PEP. Additionally, an automatic system checks registration details (name screening) across several databases and further assesses trigger risk during the ongoing monitoring process. This approach allows to identify PEPs at a very early stage of the relationship and minimizes the risk of being exposed to money laundering, bribery, and usage of illegally obtained funds.

All clients identified as PEPs during the registration process shall be flagged in our system. These individuals shall undergo continuous monitoring and regular reassessment to maintain accurate risk profiles. Enhanced Due Diligence (EDD) measures will be applied, including detailed transaction monitoring.

Given the inherent risks associated with PEPs, such clients are classified as high-risk clients. With that in mind, senior management approval for the onboarding of any PEP, or in the case of change of status of an existing client to a PEP, is mandatory. Additionally, senior management shall be ultimately responsible for the ongoing oversight of PEP relationships.

Furthermore, the Company's policy stipulates that a person will be considered a PEP for five years from the date of resignation or the end of their political role. Where the risk assessment of the particular PEP has outlined an increased risk, the period may be extended after a senior management approval, to ensure any residual risks are adequately managed.

4.5 Sanctions Screening

The imposition of economic sanctions against foreign countries remains an important instrument for the international community in the enforcement of laws relating to the financing of terrorist activity, money laundering, and fraud. Sanctions can encompass a wide variety of measures, which include limitations on official and diplomatic contacts or travel, and the imposition of legal measures to restrict or prohibit trade or other economic activity.

The Company does not accept any individuals who are listed on sanction lists. Name screening against sanctions lists is being done during the registration process by an automatic system – AgeChecked, as well as in the process of ongoing monitoring of the client. Name, surname and date of birth is being compared with Sanctions lists (OFAC, UN, EU, Canadian Sanctions List) and if customer is flagged as a match, registration is blocked, and customer is being sent to manual verification.

More details can be found in the Player Identification - Know Your Client (KYC) Policy.

5 Customer relationship

5.3 Structure of the customer relationship

In light of anti-money laundering and anti-terrorist financing policies, a customer's relationship

with the Company consists of three elements:

- **registration** - the establishment of the business relationship, including customer verification and entering into a business relationship;
- **ongoing usage** - monitoring of the player's account, followed by ongoing monitoring, including account deposits and withdrawals;
- **account closure** - termination of the relationship with the customer.

By registering on our website, customers enter into a business relationship with us. At all stages of the relationship, it is necessary to consider whether the customer is engaged in money laundering (including criminal spend) or terrorist financing.

5.4 Identification & verification

Identifying a customer means obtaining information about their identity:

- full legal name;
- full physical address;
- date of birth;
- personal telephone number;
- email address;
- identity number;

To open an account with the Company, the Player must first complete the registration process. Customers must be over allowed legal age to be permitted to register on the Website - no underage users are allowed to use the Company's services.

Verifying the identity means obtaining evidence that supports the outcome of the identifying process. Company's verification method consists of an electronic method of verification and manual verification.

5.2.1. *Player risk assessment*

Customer risk assessment starts at the beginning of the relationship. The Company recognizes the extent to which a particular customer triggers the risk factors and assesses the risk of the customer accordingly.

The Customer Risk Assessment assesses the particular risks the Company will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. The determination of the Customer Risk Rating is first assigned when a new customer applies for an account. This rating helps decide how often and in what way the customer will be reviewed in the future: the higher the risk, the more frequent and robust the ongoing monitoring of the customer would be.

The Customer Risk Assessment process takes into consideration the following factors:

CUSTOMER RISK

This involves assessing the customer's background, occupation, and transaction patterns.

Categories of customers whose activities indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders;
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures.

PRODUCT/SERVICE RISK:

This factor evaluates the risks associated with the products and services offered, including gaming products or services where customers can influence game outcomes, either on their own or in collaboration with others. Additionally, certain payment methods used by customers and accepted by casinos are seen as riskier for ML and TF. The following is a non-exhaustive list of high-risk factors:

- Anonymous payment methods (e.g. pre-paid cards and virtual assets);
- Unusual casino account usage;
- Specific game types, where bets are made even;
- Peer-to-peer gaming;
- Third-party accounts;
- Moving money from one gaming account to another;

- Multiple accounts or wallets;
- Additions or changes to associated payment methods.
- Identity fraud: Stolen financial account details used on websites, including stolen identities used to open financial accounts that are then used for gambling.
- Games with multiple operators: For example, poker platforms shared by different operators.
- Electronic wallets: Not all e-wallets are licensed in trustworthy countries, and some accept cash deposits. Moreover, e-wallets that only accept funds from financial accounts may not show the transaction to the online casino, which could help dishonest customers hide their gambling activities.

GEOGRAPHIC RISK:

This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML, CTF and CPF regulations or high levels of corruption being deemed higher risk. The nationality, residence and place of birth of the player have to be considered as these might be indicative of a heightened geographical risk. Company Name regards the following sources of information produced by the FATF and other well-known non-governmental bodies (not limited):

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML, CTF and CPF regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

Company Name consistently monitors updates to the lists above and adjusts its CDD process to reflect relevant changes.

DELIVERY CHANNEL RISK:

This factor looks at the risks associated with the methods used to establish a business relationship or through which transactions are carried out. Company Name considers the increased risk of ML/TF/PF of the use of channels that favor anonymity and interactions on a non-face-to-face basis and, to the extent possible, shall take all reasonable measures to address and mitigate said risks.

The risk assessment will categorize customers as low, medium, or high risk, with due diligence and ongoing monitoring applied proportionately:

- For customers assessed as low risk, the Simplified Due Diligence process will be applied, insofar as the customer does not display any risk-increasing elements and remains below the threshold of CWG 4,000.
- For those assessed as medium or high risk, additional information and documentation will be required in accordance with this Policy.
- Accounts classified as high risk or exhibiting potentially suspicious behaviors will be subject to review by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

As Company operates on Canadian market, risk approach shall be compliant with FiNTRAC risk assessment guidelines:

- Extreme risk – positive match with sanctions list or terrorist list, affiliated with organized crime groups/public safety risk
- High risk – foreign PEP, connection to high-risk countries (high risk countries indicated on FATF lists), high risk occupation (occupation connected with real cash operations) and consolidated lifetime deposits of CAD 25 000

- Medium risk – at least one Suspicious Transaction Report Submitted, adverse media, domestic PEP, monthly deposit more than CAD 30 000, using more than five financial instruments, minimal play or no play for up to one month after initial or subsequent deposits
- Low risk – all players that did not trigger other risk factors that justify changing the risk score

More information can be found in the Player Risk Assessment Policy.

5.2.2. Simplified Due Diligence

Where the risks of money laundering or terrorist financing are lower, Company is allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. Simplified due diligence can be used only for Low-risk players.

Examples of possible measures:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the casino can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the casino has to verify the basic identification details, while the verification of any other personal details is upon the casino, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, or when player reaches certain threshold.

5.2.3. Enhanced Due Diligence

A risk-based approach should be taken, so more thorough checks should be undertaken for higher risk customers (Extreme and High risk). The Enhanced Due Diligence (EDD) measures should be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence must be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);

- Products or transactions that might favor anonymity.
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced due diligence measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In situations presenting a higher risk of ML/TF, source of funds information must be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

5.2.4 Reliance on third parties to perform customer due diligence.

Company relies on third party software to perform automatic due diligence process (eKYC) during registration:

Registration due diligence

During registration, all data entered by the player are being passed through API call to AgeChecked. Player data are being checked against Sanctions and PEPs list, phone carrier and credit score data. If player's data are positive hit against Sanctions and PEPs list, account is blocked and sent for further manual verification. Player's identity is being checked against phone and credit score data. If it is a positive match and identity is confirmed, account can be activated. If there is no match, account is being sent for further verification.

5.2.5 Timeline for compliance and non-compliant documents

If the customer cannot provide compliant documents within 30 days from the moment the XCG 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the XCG 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

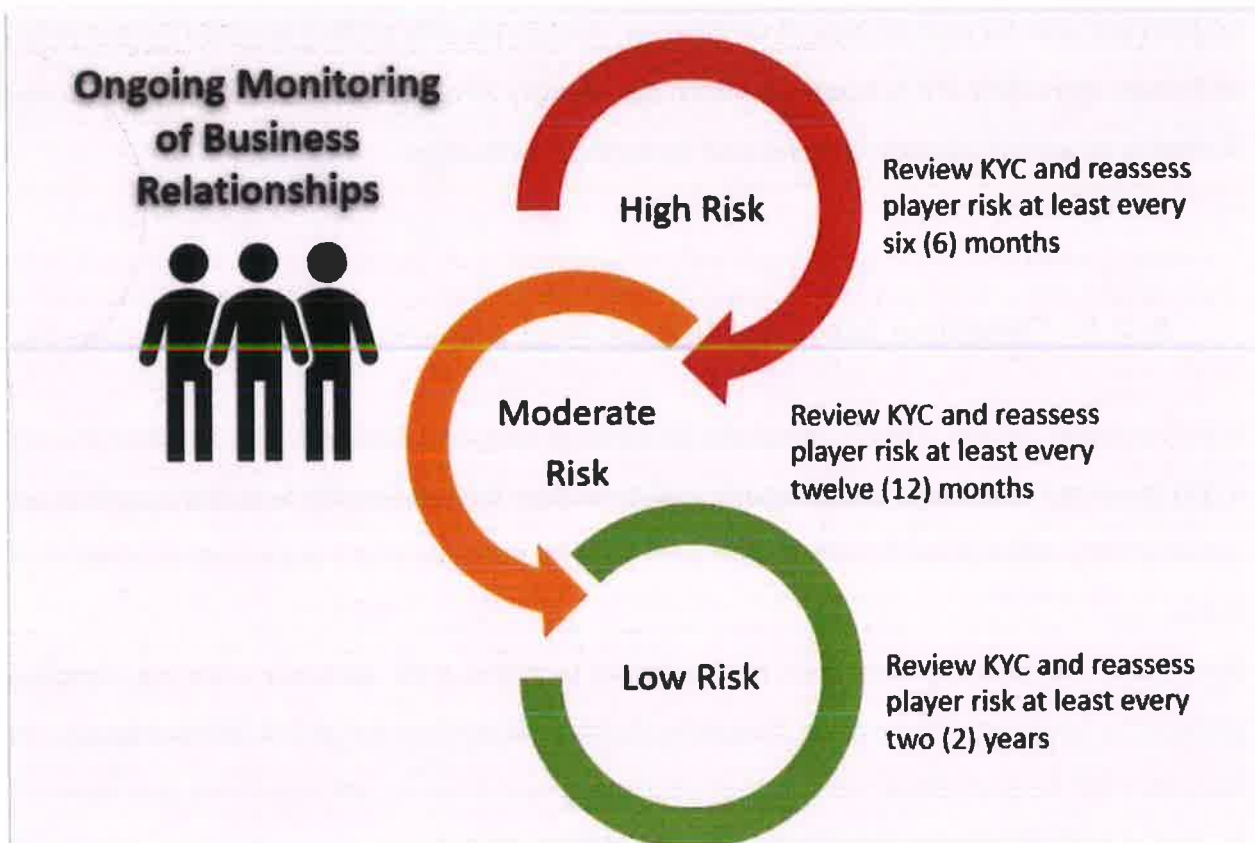
If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

5.5 Ongoing Monitoring

Monitoring of Players is carried out using the risk-based approach. Players are monitored on an

ongoing basis and assessed on a risk-sensitive basis, with extreme and high-risk Players being subjected to an enhanced ongoing monitoring conducted with appropriate frequency and depth of scrutiny:



On a day-to-day basis, Players are checked throughout the course of the relationship to ensure that transactions are consistent with the knowledge and risk profile Company holds on to the Player.

In addition, the MLRO and deputy MLRO review the existing records of Players to ensure procedures and policies are carried out correctly. Transaction monitoring rules are being reviewed at least annually.

5.6 Unusual transactions

Unusual transactions are transactions that are inconsistent with the player's profile, which can be, but not limited to:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.

- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions in the amount of CWG 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 1. A cashless transaction in the amount of CWG 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 2. Accepting or releasing a deposit in the amount of CWG 5,000 or more at the request of the client.
 3. Sale to a customer of chips in the amount of CWG 5,000 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of CWG 5,000 or more.
- Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Note: Ministerial Decree with general operation of December 1, 2015, laying down the indicators, as mentioned in article 10 of the NORUT (Decree Indicators Unusual Transactions) (N.G. 2015 no. 73).

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of CWG 5,000 or more and is considered per gaming day.

Internal reporting: Any unusual transaction must be reported internally, without any delay along with any supporting documentation.

External reporting: The compliance officer will prepare a report of all unusual transactions and report to the FIU by means of the goAML reporting portal, without any delay.

5.7 Termination of a business relationship

Circumstances when the Company may need to terminate a business relationship with a customer include:

- it is known that the customer attempted to use the relationship to launder criminal proceeds or use it for criminal spend;
- it is not possible to complete CDD or EDD checks in regard to the customer;
- if the risk score is recognized as extreme or high;
- their activity raises to an increased level of suspicion or knowledge of money laundering/terrorist financing;
- there are reasonable grounds to believe that the customer is not the identity they claim to be.

More information about the account termination can be found in the Player Risk Assessment Policy and External Reporting Policy.

5.8 Documentation of Due Diligence

The Company maintains comprehensive records of all due diligence activities, including the rationale for assigned risk levels. The CDD process is aligned with identified risks, ensuring that due diligence efforts match the customer's risk profile. All risk mitigation measures are documented and utilized during ongoing monitoring to manage potential risks effectively.

6 Risk-Based Approach

6.1 Objectives

The Company employs a risk-based approach to AML/CFT/CFP compliance, ensuring policies and procedures are proportionate to the identified risks. We periodically review risk assessment policies to keep them current and responsive to emerging threats. Further, staff training on policy updates ensures consistent application.

Client reviews are risk-based, with compliance dossiers reflecting potential risks and mitigation measures. These dossiers are updated regularly to capture changes in client risk profiles. Monitoring is based on dossier information, ensuring thorough and up-to-date oversight. Monitoring outcomes determine new risk ratings and identify emerging risks.

Regular updates and assessments in the review process promptly address changes in client risk profiles. All findings and risk rating adjustments are recorded in the compliance dossier, providing a clear audit trail for future reviews and audits.

More information can be found in the Player Risk Assessment Policy. The objectives of the Player Risk Assessment are:

- to assess a Player's ML/TF risk;
- to determine the level of due diligence required that would be appropriate with the Player's identified level of risk;
- to determine the frequency for ongoing monitoring and Player information update;

7 Regulatory Reporting

The company shall fulfil all regulatory reporting requirements - including internal and external reporting. More information can be found in the Internal and External Reporting Policies. This section outlines the process and timelines for reporting to the Financial Intelligence Unit (FIU) in Curaçao and internal stakeholders.

All employees must be vigilant in identifying suspicious activities that may indicate money laundering, terrorist financing, or proliferation financing.

7.1 Internal Reporting Procedures

Employees must report any suspicious activity immediately to the Compliance Officer using an internal reporting form. The Compliance Officer will conduct a preliminary review of the reported activity within 24 hours to determine if it warrants further investigation.

If further investigation is required, the Compliance Officer will complete this within 5 business days. During this period, the Compliance Officer may request additional information from relevant departments.

7.2 Reporting to the FIU

If the Compliance Officer determines that the activity is suspicious, an initial report must be submitted to the FIU within 2 business days of completing the internal investigation. Any additional information requested by the FIU must be provided within 5 business days of the request. The Compliance Officer will continue to monitor the reported activity and provide updates to the FIU as necessary.

7.3 Confidentiality

All reports and investigations are to be treated with the utmost confidentiality in accordance with Article 22 of the National Ordinance Reporting Unusual Transactions (NORUT). Unauthorized disclosure of information related to suspicious activity reports (SARs) is strictly prohibited and may result in disciplinary action.

8 Protection of employees and whistleblowing

Deck has established routines to protect persons who fulfil Deck's obligations

under the AML/ATF regulations.

In accordance with European Union Directive (EU) 2019/1937 (the Whistleblower Protection Directive), employees who report suspicious activities, internally or to the FIU Curaçao, in good faith are protected from retaliation. This includes protection from dismissal, suspension, demotion, harassment, and any other forms of discrimination. Company has anonymous channel for submitting such reports internally. Further information can be found in the Whistleblowing Policy.

The Compliance Officer is responsible for monitoring the effectiveness of the whistleblowing procedures and ensuring compliance with relevant legislation.

Regular reviews will be conducted to identify any areas for improvement and to ensure that the procedures remain effective and up-to-date

9 Business Affiliate and Supplier Diligence

Company recognizes that when contracting or outsourcing specific functions, there is a risk of increased AML/CFT/CFP exposure if the third parties involved are not properly vetted and their relevant processes are not assessed. Prior to entering into any service agreements that fall under this Policy, the Company performs due diligence to verify the legitimacy of the potential partners. This due diligence includes, at a minimum, establishing the identity of the party and where it concerns a legal person – of its beneficial owners and the persons authorized to represent it.

Additionally, where applicable, potential third-party suppliers are required to submit a copy of their AML/CFT/CFP policies and procedures, proof of pertinent licensing or certification. The Compliance Officer will review these documents for their accuracy and completeness

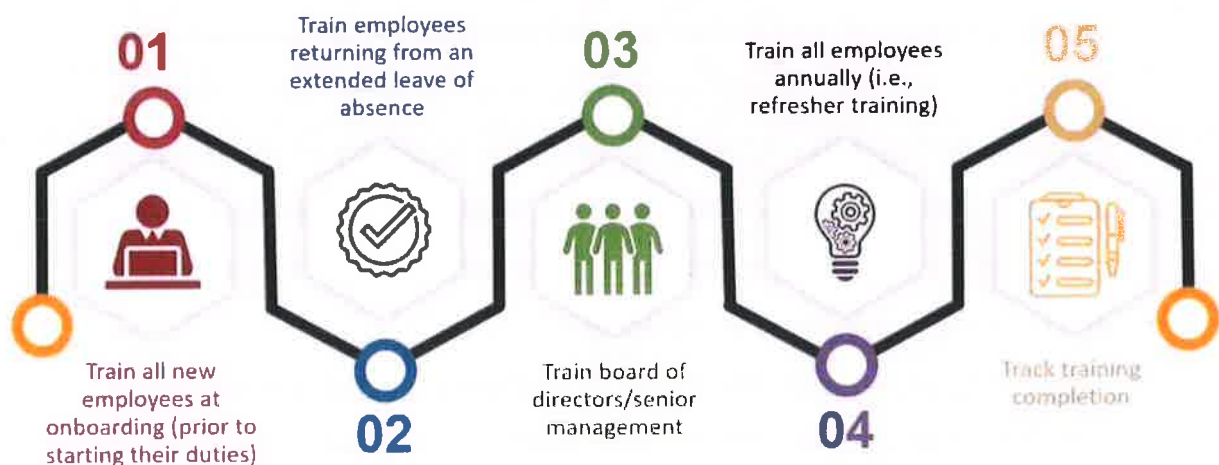
10 Training

Ongoing AML/ATF training plays a critical role in combating and preventing ML and TF risks. One of the most important controls over the detection and prevention of ML/TF activities is to have employees who are knowledgeable in ML/TF risks and who are well trained in the identification of unusual activities or transactions which appear to be suspicious.

Company employees are required to complete the training module at the time of their onboarding (prior to any Player interaction or fulfilment of any AML related activities) and on an annual basis thereafter (i.e., refresher training).

AML/ATF training must be delivered to the following employees (at a minimum) who are responsible for:

- Player onboarding and due diligence (including high-risk Player monitoring)
 - Monitoring Player transactions
 - Addressing Player queries or concerns (such as a customer service team)
 - Technology functions related to AML activities
- Training trail:



11 Independent audit function

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

11.1 Examination by the CGA

Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the CGA during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

12 Record keeping

It is essential that proper records are kept of the due diligence carried out on the customer, evidence gathered, the decisions that were made and the reasons behind them.

12.1 Types of Documents to be Retained

The following types of documents must be retained:

- Customer Identification Records: Copies of identification documents, verification data, and due diligence information.
- Transaction Records: Details of all transactions, including the amount, date, and parties involved.
- Suspicious Activity Reports (SARs): All reports submitted to the Financial Intelligence Unit (FIU) and related correspondence.
- Internal Investigation Records: Documentation of internal investigations, including findings and actions taken.
- Training Records: Records of employee training sessions, including attendance and materials used.
- Compliance Audits: Reports and findings from internal and external compliance audits.

12.2 Storage of Records

Records must be stored in a manner that ensures their integrity, confidentiality, and accessibility:

- Electronic Records: Stored in secure, encrypted databases with access controls to prevent unauthorized access.
- Physical Records: Stored in locked, fireproof cabinets within secure areas of the office. Access is restricted to authorized personnel only.
- Backup Procedures: Regular backups of electronic records must be conducted and stored in a separate, secure location to prevent data loss.

12.3 Retention Period

All records must be retained for a minimum of 5 years from the date of the transaction or the end of the business relationship, whichever is later. This period may be extended if required by law or regulatory authorities.

12.4 Secure Disposal of Records

After the retention period, records must be disposed of securely to prevent unauthorized access or disclosure:

- **Electronic Records:** Permanently deleted using secure deletion software that ensures data cannot be recovered.
- **Physical Records:** Shredded using cross-cut shredders or incinerated to ensure complete destruction.

12.5 Monitoring and Review

The Compliance Officer is responsible for monitoring adherence to these data retention procedures and conducting regular reviews to ensure compliance. Any deviations or issues must be addressed promptly.

12.6 Employee Training on Data Retention

All employees must be trained on the importance of data retention and the specific procedures outlined in this section. Training sessions will be conducted as needed to address updates or changes in regulations.

12.7 Confidentiality

All records must be handled with the utmost confidentiality. Unauthorized access, disclosure, or misuse of records is strictly prohibited and may result in disciplinary action.

Appendix I: Country Risk List

Please note that the risk classification in following list of countries is subject to continuous review. Any changes in risk indicators will be reflected promptly to ensure the list remains current and accurate.

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Bangladesh
5. Barbados
6. Belarus
7. Benin
8. Bosnia & Herzegovina
9. Bulgaria
10. Burkina Faso
11. Burundi
12. Cambodia
13. Cameroon
14. Central African Republic
15. Chad
16. China
17. Colombia
18. Cote d'Ivoire
19. Croatia
20. Cuba
21. Cyprus
22. Democratic Republic of the Congo
23. Egypt
24. Eritrea
25. Ethiopia
26. Guinea
27. Guinea-Bissau
28. Haiti
29. Hong Kong
30. India
31. Indonesia
32. Iran
33. Iraq
34. Jamaica
35. Kenya
36. Kyrgyzstan
37. Laos

38. Lebanon
39. Liberia
40. Libya
41. Mali
42. Moldova
43. Monaco
44. Mozambique
45. Myanmar (Burma)
46. Namibia
47. Nepal
48. Nicaragua
49. Niger
50. Nigeria
51. North Korea
52. Pakistan
53. Panama
54. Peru
55. Philippines
56. Russian Federation
57. Senegal
58. Somalia
59. South Africa
60. South Sudan
61. Sudan
62. Syria
63. Tanzania
64. Thailand
65. Togo
66. Trinidad and Tobago
67. Tunisia
68. Türkiye
69. Turkmenistan
70. Uganda
71. Ukraine
72. Ukraine (Crimea, Donetsk, Lugansk)
73. United Arab Emirates
74. United Kingdom
75. Vanuatu

76. Venezuela
77. Vietnam
78. Yemen
79. Zimbabwe

Low-risk countries include:

1. Australia
2. Canada
3. Denmark
4. Estonia
5. Finland
6. Germany
7. Iceland
8. Ireland
9. Luxembourg
10. Netherlands
11. New Zealand
12. Norway
13. Singapore
14. Sweden
15. Switzerland
16. Uruguay

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Curaçao
7. Czech Republic
8. Denmark
9. Estonia
10. France
11. Germany
12. Greece
13. Hungary
14. Israel
15. Italy
16. Latvia

17. Lithuania
18. Netherlands
19. Poland
20. Republic of
Ireland
21. Saba
22. Serbia
23. Sint Eustatius
24. Sint Maarten
25. Slovakia
26. Slovenia
27. Spain
28. Sweden
29. Switzerland
30. United Kingdom
31. United States of
America.

Appendix II: Business Affiliate and Supplier Due Diligence

Company information:

Registered name and legal form	
Registration number	
Date of incorporation	
Registered address	
Status	
Ultimate Beneficiary Owners (UBOs)	
Persons with significant control (directors, members of supervisory board)	
Company website (if applicable)	

The documents below must be duly certified (where applicable) and, if they are not in the English language, provided with legalized translation in a language understandable by the Company Name:

Document	Remarks
Certificate of Incumbency showing the Ultimate Beneficial Owner(s) and Director(s)	
Recent Excerpt from the Chamber of Commerce or equivalent	
Certified copy passport of UBO(s) and Director(s)	
Proof of address of the UBO(s) and Director(s) no older than 3 months ¹	
Proof of Licensing	
AML Policy	

Appendix III: Internal Unusual Activity Report

¹ For natural persons who live or reside outside of Curaçao, and who are not personally identified by the provider, the NOIS mandate that the identity is established by either (1) a photocopy of an identification document (e.g. passport, ID card, driver's license) accompanied by a certified copy or extract from the Civil Registry of the person's place of permanent residence, or (2) following electronic receipt of an identity document of the individual, within 2 weeks we receive a certified copy of the document.

Date of report:

Client ID:

Date of account registration:

Account status (Active/Suspended/Blocked):

Risk rating:

Account balance:

Client details:

Full name:

E-mail:

Phone number:

Brand registration:

Date of birth:

Nationality/Country of registration:

Address:

Due diligence documents held:

Reason for reporting:

< explain what activity / transaction gave rise to the report >

Date of unusual activity/transaction:

Provide details (e.g. dates and amounts) of any known intended or pending transactions:

Reporting employee:

Signature:

Date:

Upon completion, please forward the form to the Compliance Officer as soon as possible.

