

Continent Gaming N.V.

AML Policy

Internal version

A handwritten signature in black ink, appearing to be 'J. van der...'.

August 2025

AML Policy

Summary

Abbreviations.....	3
Definitions	3
Regulations.....	5
Scope	5
Introduction.....	6
Money laundering and terrorist financing risk assessment	7
Risk based approach	7
Business Risk Assessment (BRA)	8
Customer Risk Assessment (CRA)	9
Risk factors specific to the Gambling Sector.....	9
Technological developments risk assessment	11
Customer identification and due diligence	12
Scope	12
The CDD measures	13
Identification and verification of the Customer	14
Identification and verification of the Beneficial Owner	15
Assessing and obtaining information on the purpose and intended nature of the business relationship	16
On-Going Monitoring	17
Timing of CDD Measures.....	18
Enhanced Due Diligence.....	19
Simplified Due Diligence	19
Politically Exposed Persons	20
Application of CDD measures to existing customers	21
The termination of the business relationship	21
Reliance on third parties to perform customer due diligence	21
Reporting of unusual transactions	22
Reporting obligations	22
Prohibition of disclosure	24
Record Keeping.....	25
Anti-Money Laundering Compliance Program.....	25
Introduction.....	25

AML Policy

A system of internal policies, procedures and controls.....	26
The Compliance Officer: appointment and responsibilities	28
Screening of and appropriate training plans and programs for personnel.....	29
An independent audit function to test the AML program.....	31
Examination by the Curacao Gaming Authority.....	32
Appendix 1. Countries list	33

Abbreviations

1. AML – Anti-Money Laundering
2. CDD – Customer Due Diligence
3. CFT – Combating the Financing of Terrorism
4. CFATF – Caribbean Financial Action Task Force
5. CGA – Curacao Gaming Authority

Definitions

Casino

In this policy - online casino.

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 management level and independent from the games operations, responsible for the detection and deterrence of money laundering and terrorist financing.

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 financing of proliferation of weapons of mass destruction

FATF Recommendations

A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions

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

FIU

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

Kingdom Sanctions Act

AML Policy

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

NOIS

National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT

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

Other online games

Includes sports betting, esports-betting, fantasy sports, lottery and bingo, skill-based games and virtual sports.

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, judicial or military officials, senior executives of state owned corporations, 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, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Sanctions National Ordinance

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

Source of Funds

Refers to how the funds for a particular transaction were obtained by the Customer, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, 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, business ownership interests.

AML Policy

Unusual transaction

A transaction that is considered as such based on certain indicators, pursuant to Article 10 of the NORUT.

(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.

Regulations

1. The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92);
2. The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99);
3. Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as
4. mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
5. Sanctions National Ordinance (N.G. 2014, no. 55);
6. Kingdom Sanction Act (N.G. 2016, no. 54);
7. National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
8. 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);
9. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2
 - a. of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
10. 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);
11. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
12. The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

Scope

1. This Manual is a guideline for Continent Gaming N.V., (hereinafter called 'the Operator')

AML Policy

in creating an efficient business process and provides clarity to the Operator's rules and internal controls included within the procedures. It enables the Operator to 'operationalize' documents such as regulation, compliance, and policies and establishes the rules that all employees have to follow while performing their duties and responsibilities related to AML Law. It assists the Operator to address in an effective way the legislative and regulatory requirements.

2. This Manual is primarily intended to be used electronically; however, it is recognized that the Manual may be required to be used using non-electronic means such as a hard copy or a printout.
3. This Manual is fully compliant with the AML/CFT legislation of Curacao, includes international best practices and requirements of international directives included crypto asset legislation.
4. This manual applies to transactions with both virtual currency and fiat currency.
5. This Manual is developed by the Compliance Officer and approved by the Senior Management. It should be reviewed at least annually and amended from time to time according to changes in legislation and/or guidelines issued by CGA.

Introduction

1. All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:
 - Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. 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 requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
 - Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. 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;
 - Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.
2. Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but

AML Policy

the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

3. 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.
4. Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. All natural and legal persons in Curaçao are required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. This is to comply with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act.

The operator must have a mechanism to check the sanction status of a withdrawing participant so that a sanctioned person or organization cannot remove money from an account that should be frozen. In such cases, a report must be filed with the FIU and the casino has to take the 'Process for the freezing of resources' into account.

5. Involvement in money laundering, whether knowingly or unknowingly, may result in criminal liability and severe reputational damage to the Operator and its Senior Management, officers and staff. The Operator, therefore places the utmost importance on complying with all applicable laws and regulations for the prevention of money laundering and will use the procedures set out in this Manual to prevent its business from being abused for such criminal activities.

Money laundering and terrorist financing risk assessment

Risk based approach

1. The Operator shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of ML/CTF appears to be comparatively higher.
2. A risk-based approach to AML/CFT means that the Operator is expected to identify, assess and understand the money laundering and terrorist financing risks to which it is exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. The risk-based approach starts with the identification, recording and

AML Policy

assessment of the risk that has to be managed. The Operator needs to assess and evaluate the risk of how it might be potentially exposed or vulnerable by its services by criminals for the purpose of money laundering and terrorist financing.

3. Applying Risk-based Approach means that the Operator has to:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

4. The Operator should risk assess its business activity (Business Wide Risk Assessment) and the risk to which it is exposed as a result of business relationships or occasional transactions (Customer Risk Assessment). The Business Wide Risk Assessment is necessary for the Operator to understand the overall exposure of its business to money laundering/terrorist financing and to identify areas of business it needs to prioritize in the fight against money laundering and terrorist financing. The Customer Risk Assessment is necessary to understand its money laundering and terrorist financing risk exposure that is a result of a business relationship or occasional transaction.

5. The Operator should always identify and assess the money laundering and terrorist financing risks associated with the following groups of risk factors as a minimum:

- products, services and transactions it offers,
- countries or geographic areas,
- the customers it attracts, and
- delivery channels it uses to service its customers.

Business Risk Assessment (BRA)

1. The steps taken for identification and assessment of money laundering and terrorist financing risk must be proportionate to the nature and size of the Operator. In this regard, the Operator must:

- keep an up-to-date record in writing of all the steps taken to identify and assess the money laundering and terrorist financing risks to which its business is exposed;
- provide the written risk assessment it has prepared and the information on which it was based to the CGA on request.

2. The BRA must be reviewed and updated at least annually and every time that there is a material change influencing the Operator's business – e.g. changes in regulation, introduction of new products/services, new technology, delivery channels etc.

3. The BRA should be signed-off at the Board level and needs to be kept up to date. Once the BRA has been completed, the Operator should be in the position to set a "risk-

AML Policy

- appetite” which means that the Operator decides the level of risk it is prepared to accept.
4. In order to work risk-based, the Operator has to continuously follow the latest reporting regarding money laundering and terrorist financing.

Customer Risk Assessment (CRA)

1. Customer Risk Assessment should be completed in the context of a business relationship or occasional transaction and lead to categorization of customers and occasional transactions as low, medium or high risk.
2. The assessments of risk should be based on criteria that reflect the causes of risk and should be documented properly. Corresponding Customer Due Diligence measures, periodic monitoring and controls should accompany each category of risk. A Customer Risk Assessment for every business relationship and occasional transactions should be documented accordingly and the Operator should be able to provide the CGA with evidence that its Customer Due Diligence measures are commensurate with the risk level.
3. The Customer Risk Assessment will assess the particular risks the Operator 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. On the basis of the CRA can be applied the proper level of CDD.
4. The Operator must establish and maintain policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's risk assessment of money laundering, terrorist financing and proliferation of weapons.

Risk factors specific to the Gambling Sector

Customer risk

1. Customer risk is the risk of ML/TF that arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of customers whose activities may indicate a higher risk include:
 - Customers who have multiple sources of income;
 - Customers with irregular income streams;
 - PEPs;
 - High spenders (money can be derived from illegal activities);
 - Disproportionate spenders (inconsistent with the Operator's information about customer's known source of income/assets);
 - Casual customers like locals/tourists, especially when spending pattern changes;
 - 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;
 - Multiple casino player rating accounts to hinder the Operator to track their gambling activities;
 - Unknown customers (redeeming large amounts of chips);
 - Junkets (junket operators monitor player activity and issues and collect credit).

AML Policy

2. The Operator must set a value which represents the upper value of a typical Customer's transactions. The Customer having a single source of regular income will pose a lesser risk of ML/TF than the Customer who has multiple sources of income or irregular income streams.

Country/geographic risk factors

3. Some countries pose inherently higher money laundering and terrorist financing risk than others. The Operator should utilize a variety of credible sources to determine a level of money laundering and terrorist financing risk related to a specific country. In this regard, the Operator needs to take into consideration as a minimum the risk factors provided in the Law and Guidelines issued by CGA.
4. When identifying the geographic risk associated with countries and geographical areas related to a particular customer, the Operator should consider the risk related to:
 - the jurisdictions in which the customer and any beneficial owner are based;
 - the jurisdictions that are the customer's and any beneficial owner's main places of business;
 - the jurisdictions to which the customer and any beneficial owner have relevant personal links.
5. When assessing country/geographic risk the Operator should as a minimum consider any association with financial sanctions orders, quality of controls, terrorism risk and levels of corruption or other criminal activity related to the country/geographic area.
6. The Operator should take into account a variety of sources of information produced by the FATF and non-governmental well-known bodies:
 - 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/CFT regime;
 - Countries sanctioned by the OFAC (Office of Foreign Assets Control, US);
 - 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.

The list of countries that are considered as high risk and low risk has given in Appendix 1.

Product, service and transaction risk.

7. Some products or services are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the

acceptance by the Operator of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of the Operator accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g. roulette, craps → even bets);
- Peer to peer gaming;
- The use by customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to financial institution accounts to fund the Operator account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Games involving multiple operators (Poker on platforms shared by multiple operators);
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

Delivery channel risk factors

8. When identifying the risk associated with the way in which the customer obtains the Operator's products or services, the Operator should consider the risks related to:
 - anonymous channels that increase the risk of ML/FT;
 - the extent to which the business relationship is conducted on a non-face-to-face basis;
 - any introducers or intermediaries the Operator might use and the nature of their relationship with the Operator.

Technological developments risk assessment

1. The Operator should maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It should identify and assess the money laundering or terrorist financing risks that may arise whenever:
 - a new product is developed;
 - a new business practice emerges;

AML Policy

- a new delivery mechanism becomes available;
 - a new or developing technology is used for both new and pre-existing products.
2. In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Risk assessments must be documented.

Customer identification and due diligence

Scope

1. The CDD measures must enable the Operator:
 - to identify the customer and verify that customer's identity using reliable, independent source documents, data or information;
 - to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner;
 - to understand and, as appropriate, to obtain information on the purpose and intended nature of the business relationship;
 - to conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Operator's knowledge of the customer and his/her risk profile, including, where necessary, the source of funds.
2. The customer's risk profile is essential to allow the Operator to apply a certain level of Customer Due Diligence commensurate to the identified ML/TF risk. The purpose of collecting information is to provide the Operator with documentation to assess the risk that may be associated with the Customer and to build a customer profile to assess how the Customer is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior. 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 money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.
3. The Operator should undertake Customer Due Diligence (CDD) measures when:
 - establishing business relations;
 - carrying out occasional VA transactions above the monetary equivalent of NAf. 4,000;
 - carrying out occasional fiat transactions above the monetary equivalent of NAf. 4,000;
 - there is a suspicion of money laundering or terrorist financing; or
 - the Operator has doubts about the veracity or adequacy of previously obtained customer identification data.

AML Policy

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of NAf. 4,000.

4. In case the Operator carries out an occasional transaction above the monetary equivalent of NAf. 4,000, it is still obliged to apply CDD measures. The Operator is also subject to this obligation when they execute a series of linked transactions which, though individually below the applicable threshold, would cumulatively meet or exceed the NAf. 4,000 threshold. Transactions are considered as linked if for example they are carried out by the same Customer through the same game or in one gaming session.

The CDD measures

1. Customer Due Diligence measures consist of:
 - identifying the customer;
 - verifying the customer's identity;
 - where there is a beneficial owner who is not the customer, identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner so that the Operator is satisfied that it knows who the beneficial owner is;
 - assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship;
 - conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that:
 - the transactions being conducted are consistent with the Operator's knowledge of the customer and the risk profile
 - their source of funds and
 - documents, data or information held are kept up to date.
 - Where a person claims to act on behalf of a customer, the Operator must:
 - verify that the person is authorized to act on the customer's behalf;
 - identify the person;
 - verify the person's identity on the basis of documents or information which, in either case, is obtained from a reliable source which is independent of both the person and the customer.
2. The Operator, its director, officer and employees are prohibited to disclose the fact that an UTR is being reported to the FIU. A risk exists that Customers could be unintentionally tipped off when the Operator is seeking to perform its CDD obligations in these circumstances. If the Operator reasonably believes that performing the CDD process will tip-off the Customer, it may choose not to pursue that process, and should file an UTR to the FIU.

Identification and verification of the Customer

1. Identification refers to the collection of personal details of the Customer to establish the identity of the Customer. Verification consists in confirming the personal details collected for identification purposes using reliable, independent source documents, data or information.
2. Identification of the Customer. The Operator should identify the customers who are natural persons by obtaining the following information:

- True name and/or names used;
- Full permanent address, including postal code;
- Government issued document number, issuing date and country;
- Telephone number;
- E-mail address;
- Date and country of birth;
- Nationality;
- Details on the profession and other occupations of the customer including the name of employer/business.

Note: In low risk scenarios the Operator may limit identification to the three personal details. In high risk situations, it is possible that the Operator considers the collection of additional personal details as necessary to mitigate the higher risk of ML/FT.

3. The identity of a natural person shall be established through one of the documents, valid in the country of issue, listed in art. 3, par. 1, of the NOIS:

- driver's license,
- an identity card,
- a travel document or passport,
- another document to be designated by the Minister.

If the natural person lives or stays abroad, the following will suffice:

- a photocopy of one of these documents, provided that it is accompanied by a certified copy or extract of the Civil Registry of the place of residence or residence of the client,
- the transmission of any of the aforementioned documents by electronic means, provided that the service provider receives a certified copy of the document sent within two weeks of electronic receipt thereof.

Note: Under the conditions, mentioned in art. 3, par. 1, second section, and par. 7, of the NOIS it is allowed to establish the identity of the natural person by other means.

4. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

AML Policy

Verification of identity has to be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g. passport, identity card).

For verification of the Customer's residential address, the Operator can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. Verification can also be done by checking social media, telephone directories, companies' registries or media and news sources.

Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. If the Operator obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly where the type of document is unfamiliar.

The Operator should recognize that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, the Operator should take practical and proportionate steps available to establish whether the document offered is a forgery or otherwise false. Commercial software is available to check the validity of passports of any country that issues machine-readable passports.

If satisfied that the original and genuine identification documents have been presented, the Operator should keep copies of the pages containing all relevant information which must be certified as true copies of the original documents by the Operator's employee who verified the identity of the customer.

5. Sanctions screening and PEP status screening.

All Customers should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the Operator should also take that local list into account. The Operator must ensure it does not do business with customers that are subject to international sanctions.

Before doing business or performing an occasional transaction for the first time with the Customer, the Operator should check published lists of known or suspected terrorists or other sanctioned persons or companies:

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists | Office of Foreign Assets Control (treasury.gov);
- EU Sanctions List <http://www.sanctionsmap.eu/#/main>.

Identification and verification of the Beneficial Owner

1. The Operator are required to identify and verify the identity of the beneficial owner. The Operator should make sure that customers are registering an account to play and transact on their behalf.
2. For the purpose of this Direction "beneficial owner" means any natural person(s) who

AML Policy

ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted.

3. If business model will include registered player accounts used by companies (corporate accounts), the applicable beneficial ownership requirement will relate to the beneficial owners of the companies registering those accounts. The Operator will develop separate procedures for identification and verification of the Beneficial Owner.

Assessing and obtaining information on the purpose and intended nature of the business relationship

1. The Operator must understand the purpose and intended nature of the business relationship or transaction in order to assess whether the proposed business relationship/transaction is in line with the Operator's expectation and to provide the Operator with a meaningful basis for ongoing monitoring.
2. Depending on the Operator's risk assessment of the situation, information that is relevant must include as a minimum the following:
 - the anticipated turnover/size of transactions and kind of wagering activities in which the customer is likely to engage;
 - the origin of funds;
 - the source and size of the customer's wealth and annual income;
 - regularity or duration of the relationship.
3. If the risk of ML/FT is high or the Operator have doubts as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation.
4. In developing a customer risk profile, the Operator should consider using statistical data to develop behavioral models against which to gauge a customer's activity rather. The Operator can use data collected from the Central Statistics Department such as average national income, average disposable income etc. These indicators should allow the Operator to determine the average wagering power of the Customers from a given jurisdiction.
5. The use of statistical data is incompatible with high-risk situations as the transactional pattern will fall outside the average behavioral model. In such circumstances, the Operator have to collect source of wealth information.
6. The Operator shall develop risk profiles to determine the customer categories, which expose the Operator to higher risk.
 - Low-risk category includes the following customers:
 - countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems;

AML Policy

- countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity
- Medium-risk category includes the following customers:
 - Any customer not falling under either high-risk or low-risk category.
- High-risk category includes the following customers:
 - customer risk factor:
 - a. business relationship is conducted in unusual circumstances;
 - b. the customer or the Beneficial owner of the customer is a PEP;
 - c. 'Customer accounts' in the name of a third person;
 - d. Customers convicted for a Predicate;
 - e. Customers from countries which inadequately apply FATF's recommendations;
 - f. Other Customers that their nature entail a higher risk of ML/TF;
 - g. Any other customer determined by the Operator itself to be classified as such;
 - country risk factors:
 - a. countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems;
 - b. countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
 - c. countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations;
 - d. countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operation.

On-Going Monitoring

1. The Operator shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Operator's knowledge of the customer, their risk profile, including where necessary the source of funds.

Ongoing monitoring of identity

2. In conducting ongoing due diligence on the business relationship, the Operator should hold accurate and up to date identification data of its customers. The Operator has to obtain evidence of identity periodically to detect any changes, refresh the data on key events (i.e. change of payment instrument) and has to tracking expiry dates on evidence of identity and refreshing it as it expires. The Operator has to determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Ongoing monitoring of transactions

3. Transaction monitoring is executed to prevent involvement of the Operator with ML/TF and to safeguard its reputation. If customer's transactions are not consistent with what the Operator knows or expects from the customer, the Operator has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction. The Operator has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction.
4. After receiving this information the Operator has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.
5. For customers using VA information must include:
 - IP address with an associated time stamp;
 - geo-location data;
 - device identifiers;
 - VA wallet addresses;
 - transaction hashes.

If the Operator uncovers VA addresses that it has decided not to establish or continue business relations with or transact with due to suspicions of ML/TF, the Operator should consider making available its list of "blacklisted wallet addresses," subject to the laws. The Operator should screen its customer's and counterparty's wallet addresses against such available blacklisted wallet addresses as part of its ongoing monitoring.

Timing of CDD Measures

1. A business relationship is a business, professional or commercial relationship between the Operator and a customer, which is linked to the professional activities of the Operator and is expected by the Operator, at the time of its establishment, to have a certain duration.
2. In the context of the Operator, a business relationship occurs when:
 - a customer opens an account with the Operator;
 - a customer becomes a loyalty member (when a membership scheme is operated by the Operator);
 - a customer applies for or is granted a credit facility at the Operator;
 - a customer sends front money to the Operator;
 - the Operator uses an e-wallet provider to bring money with the purpose of gaming (in which case a business relationship with the e-wallet provider is established).
3. The Operator has to verify of identity be conducted when engaging in financial fiat transactions equal to or in excess of NAF. 4,000. CDD measures must have been conducted at the time the threshold is reached. The Operator are required to apply a minimum level of CDD measures prior to reaching the threshold. The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the Customer since

AML Policy

the establishment of the business relationship, including any peer-to-peer transfers. Once the threshold is reached, the Operator has to conduct PEP status screening and carry out a customer risk assessment and meet their remaining CDD obligations.

4. In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the Operator obtains any necessary information from the customer concerned. When the Naf. 4,000 threshold is reached, the Customer cannot deposit funds into the account or withdraw funds from the account.
5. If the requested information and documentation is not received within 30 days from the moment the Naf. 4,000 threshold was met in order for the Operator to complete CDD, it has to terminate the relationship with the Customer and report the transaction to the FIU.

Enhanced Due Diligence

1. Enhanced Due Diligence has to 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.
2. The applied measures must be consistent with the risks identified. 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 Customer. 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.
3. In situations presenting a higher risk of ML/TF, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

Simplified Due Diligence

1. Where the risks of money laundering or terrorist financing are lower, the Operator is allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. Examples of possible measures:

AML Policy

- 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 Operator to obtain the Customer'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 Operator can also use alternative reputable information sources, even where these do not contain photographic evidence of the Customer's identity (e.g. birth certificates, bank statements etc.);
 - The extent of personal details verified can also vary. In low-risk situations, the Operator has to verify the basic identification details, while the verification of any other personal details is upon the Operator, 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.
2. Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Politically Exposed Persons

1. The Operator must apply Enhanced Due Diligence measures with respect to transactions or business relationships with PEPs. The definition of a PEP includes family members of such person and persons known to be close associates of such person.
2. The Operator is required to have in place appropriate risk procedures and management systems to determine whether the customer or the beneficial owner of the customer is a PEP.
3. In cases of business relationships or transactions with PEPs the following Enhanced Due Diligence measures must be applied:
 - obtain Senior Management approval for establishing/continuing business relationships with such persons or performing a transaction;
 - take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons. This would mean obtaining documentary evidence of source of wealth and source of funds;
 - conduct enhanced ongoing monitoring of those business relationships.
4. Where a PEP is no longer entrusted with a prominent public function, the Operator shall, for at least 12 months, be required to consider the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to PEPs.
5. The customer due diligence has to be tailored to the risk of the PEP, where the following is taken into consideration:
 - the type of public function of the PEP;

AML Policy

- the country from which the PEP originates;
 - the transactions that the PEP carries out.
6. Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the Operator must regularly screen for PEP status during the business relationship. Should the Customer who had not been identified as a PEP at onboarding stage result to have become one, the Operator is required to implement the measures described above within the thirty-day window. Failing with these, will result in the Operator to terminate the relationship with this customer.

Application of CDD measures to existing customers

1. The operator should apply CDD measures to existing customers based on materiality and risk and conduct due diligence on such existing relationships at the appropriate time. The operator must periodically audit existing procedures, revise them when legislation changes, and implement best practices.

The termination of the business relationship

1. In case the obligations arising from the customer due diligence cannot be met, the Operator cannot establish the business relation or perform the transaction or he is obliged to terminate the business relationship with the Customer. The Operator must also keep a record of all the attempts made to get the necessary information and documentation. To this end, the Operator may decide to either close the account or to keep it blocked and suspended in its entirety.
2. In the event that the Customer makes the requested information and/or documentation available to the Operator following the closure or the suspension and blocking of the gaming account, the Operator has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.
3. The Operator is to consider whether there are any grounds giving rise to suspicion of ML/TF/FP. The reluctance of the Customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. The Operator should consider all factors and information it has at his disposal to decide whether there are grounds to suspect ML/FT/FP. If, however the presumption of ML/FT/FP exist the Operator should submit an unusual transaction report to the FIU with regard to this player.
4. Where there is no reason for the retention of funds, the funds are to be remitted back to the Customer. This has to be done through the same channels used to receive the funds.

Reliance on third parties to perform customer due diligence

1. Gambling companies may rely on third parties when performing all elements of the CDD measures, provided that the criteria set out below are met. The third party should be subject to CDD and record-keeping requirements. The third party will have an existing business relationship with the Customer, which is independent from the relationship to be formed by the Customer with the relying institution. Where such reliance is permitted,

the ultimate responsibilities for CDD measures remains with the Operator relying on the third party. The criteria to be met are as follows:

- The Operator has to obtain the information concerning all elements of the CDD measures immediately from the third party it is relying upon;
 - The Operator should have an agreement with the third party being relied upon that copies identification data or other relevant documentation relating to CDD requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. The Operator, however, remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring;
 - The Operator should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements as described in this regulation. The third party will have an existing business relationship with the Customer, which is independent from the relationship to be formed by the Customer with the relying institution, and would apply its own procedures to perform CDD measures;
 - When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.
2. The Operator should be periodical assessments of how the service provider is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively. The decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

Reporting of unusual transactions

Reporting obligations

1. Gambling companies are required to detect and report either intended or completed unusual transactions. The Operator must have adequate procedures in place that cover the following:
- The recognition of unusual transactions;
 - The documentation of unusual transactions; and
 - The reporting of unusual transactions.

Recognition of unusual transactions

1. An unusual transaction is a transaction that does not match the Customer's profile. The operator must collect documentation to assess the risk that may be associated with the Customer and build the Customer profile to assess how the player intends to act within the business relationship.
2. NORUT legislation establishes objective and subjective indicators by which casinos must assess whether the Customer's transaction qualifies as an unusual transaction.

AML Policy

3. The Operator must provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions.
4. The staff must report to the compliance officer about all these unusual transactions in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements.
5. The compliance officer must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the Operator, the reason shall be adequately documented and signed off by the compliance officer and/or management.
6. The following transactions or intended transactions are deemed unusual:
 - 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 NAf. 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:
 - A cashless transaction in the amount of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the Operator to a local or international bank account, at the request of the client.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
 - Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of NAf. 5,000 or more;

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 NAf. 5,000.

- 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.

Reporting of unusual transactions

1. By virtue of article 11 of the NORUT, the Operator must report unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, they should have clear procedures for internal and external reporting of unusual transactions in place. These should be communicated to their personnel.
2. The Operator shall be responsible for the identification and reporting to the FIU of transactions that can be qualified as unusual transactions.
3. By virtue of art. 11, third paragraph, of the NORUT, the Operator shall examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic

AML Policy

or lawful purpose, in order to decide whether or not to report the transactions as unusual transaction to the FIU.

The Operator shall maintain records, containing the information and documentation necessary to decide whether or not to report the transaction or pattern of transactions to the FIU, for at least five years after the business relationship is ended, or after the date of the occasional transaction or transaction pattern).

Such records must be sufficient to permit 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.

4. All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

The documentation of unusual transactions

1. The Operator has to register with the FIU and to get access to the go AML reporting portal after validation by the FIU.
2. The compliance officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Operator shall report to the FIU the details of the transactions by means of the go AML reporting portal. The reports and the submission of the thereto related information (all supporting documents) should be done in English.
3. The Operator shall record each unusual transaction individually on a Reporting Form. Individual Reporting Forms are numbered sequentially. Any Reporting Form that is voided shall be retained by the Operator.
4. Each report about an unusual transaction will include at least the following information:
 - the identity of the client;
 - nature and number of the identification document of the client;
 - the nature, date, time and place of transaction;
 - the amount, destination and origin of the funds, or other values involved in the transaction;
 - the circumstances that identified the transaction as unusual.
5. The Operator and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

Prohibition of disclosure

1. The Operator and its senior management and employees shall not disclose any details or information to the customer nor to third parties in connection with a report filed to the FIU or a request for information made by the FIU. The Operator should increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

Record Keeping

1. The Operator shall maintain records, containing the information and documentation necessary to decide whether the objective of the CDD measures referred to in art. 7, paragraphs 1 and 3, of the NOIS was met, and to establish the background and purpose of transactions, for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Such records must be sufficient to permit 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.

Note: Such records may have been obtained through e.g. CDD measures (copy of identification documents, name, address and place of residence of the client, the nature, number and date and place of issue of the identification document, the nature of the service, the nature, origin, destination, the size and other unique features of the values involved) individual transactions, member account files and business correspondence, including the results of any analysis undertaken.

2. The Operator is obliged to record the following data in such a way that they are accessible:
 - the name, address and place of residence or place of establishment of the client and the ultimate interested party if there is one and of the person in whose name the deposit or account is made, the person on whose behalf a payment or transaction is made, as well as of their representatives, in the VA context, this could mean the “wallet address” of the VA;
 - the nature, number and date and place of issue of the document used to establish identity;
 - the nature of the service.
3. VASPs must submit the required information to the Operator immediately and securely. “Immediately,”— given the cross-border nature, global reach, and transaction speed of VAs—means that providers should submit the required information prior, simultaneously or concurrently with the transfer itself. “Securely”, is meant to convey that providers should transmit and store the required information in a secure manner. This is to protect the integrity and availability of the required information to facilitate record-keeping (among other requirements), facilitate the use of such information by receiving VASPs or other obliged entities and protect the information from unauthorized disclosure.
4. The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

Anti-Money Laundering Compliance Program

Introduction

1. An anti-money laundering program is an essential component of the Operator’s compliance regime. The primary goal of the program is to protect the Operator against

AML Policy

money laundering and to ensure that the Operator is in full compliance with relevant laws and regulations. The AML program is risk-based and is designed to mitigate the money laundering and terrorist financing risks the Operator may encounter. The AML program establishes minimum standards for the organization that are reasonably designed to comply with applicable laws and regulations.

2. The anti-money laundering program ensures that the obligations regarding customer due diligence, reporting unusual transactions, retention periods, data protection and training are met. The Operator tests the anti-money laundering program systematically and adapts the program to the current risks that arise within the company's own organization. The AML program has the approval of senior management.

A system of internal policies, procedures and controls

1. The Operator's Board of Directors and Senior Management bear the final responsibility for ensuring that it applies an effective system to prevent money laundering and terrorist financing as well as responsibility for creating the culture of compliance. They have the ultimate responsibility to ensure that appropriate and effective systems and procedures for internal control have been introduced and applied, which reduce the risk of the products and services of the Operator being used for money laundering and terrorist financing.
2. The Operator must appoint a competent member of the Board of Directors, to be personally responsible for the implementation of the provisions of the Law and relevant AML/CFT Directives and/or circulars and/or regulations, including any relevant acts, Directives and Regulations.
3. It is required that the Operator's responsible director will be the Board level executive responsible for the Operator's compliance with the Law, this Direction, any applicable acts, Directives and Regulations and direction and the effectiveness of Operator's risk management arrangements. They will be responsible for the supervision of the Compliance Officer and the implementation of the Law and Directions as well as any other applicable regulations.
4. The Operator is required to establish the following measures, procedures and controls:
 - The Board of Directors will define, record and approve the general principles of the Operator's policy for the prevention of money laundering and terrorist financing, which it communicates to Senior Management and the Compliance Officer. An effective program for the prevention of money laundering and terrorist financing requires a recorded and clear message in relation to the risk appetite, which will determine the expectations, parameters and limits of operation of the program and the Operator's commitment to combatting money laundering and terrorist financing.
 - The Board of Directors should give leadership by expressing the Operator's values and corporate compliance culture ensuring that its AML program behavior reflects these values.
 - The Board of Directors and the Senior Management should have knowledge of the level of risk of money laundering and terrorist financing that the Operator is exposed to, so as to decide whether all necessary measures are being taken for its management, according to its risk appetite.

AML Policy

- The Board of Directors designates an experienced person to the position of the Compliance Officer have, and continually acquire the required knowledge and skills for their roles.
- There needs to be clear access and reporting mechanisms between the responsible executive and the Compliance Officer for escalated incidents and monitoring the activity to manage money laundering and terrorist financing risk.
- The Board of Directors and Senior Management shall ensure that policies, procedures and measures are applied across the Operator business activities so as the risk of money laundering and terrorist financing is identified, assessed and managed during the day-to-day operations of the Operator and in relation to:
 - The development or introduction of new products, services, new business practices, including new delivery channels, new financial management arrangements, including contracts with affiliates or associates,
 - The use of new or developing technologies relating changes in existing products or their delivery, and
 - Possible changes in the business model of the Operator.

Note: Risk assessments should take place prior to the launch of the new/ changed products, business practices or the use of new or developing technologies.

- The Board of Directors and Senior Management shall ensure that proper governance arrangements, reporting and information management arrangements for managing money laundering and terrorist financing risk are in place and are based on the three lines of defence model with clear definition of the responsibilities of each department involved in the prevention of money laundering and terrorist financing.
- The Compliance Officer is responsible in cooperation with other departments for designing policies, procedures and controls and also the description and clear definition of responsibilities and limits of responsibility of each department that is dealing with matters related to the prevention of money laundering and terrorist financing and to ensure that the internal practices, procedures and controls are appropriately documented.
- The responsible director and Senior Management shall approve the AML/CFT policies and procedures and ensure this is effectively communicated to all managers and employees that manage, monitor or control the customers' transactions with responsibility for the application of the practices, measures and procedures determined.
- The Board of Directors shall assess and approve the Compliance Officer's Annual Report and shall take all actions as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.
- The Board of Directors and Senior Management shall ensure that all requirements of the Law are applied and that the Operator is able to assure the CGA with evidence that appropriate, effective and sufficient systems and controls are present for achieving the identification and management of money laundering and terrorist financing risk.
- All employees should made aware of the person appointed as the Compliance Officer to whom they shall report information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing.

AML Policy

- The Board of Directors and Senior Management shall receive sufficient, regular and objective information to have an accurate picture of the money laundering/terrorist financing risk to which the Operator is exposed.
- The Board of Directors and Senior Management shall receive sufficient and objective information from the Compliance Officer and Internal Audit regarding the effectiveness of the measures and controls against money laundering and terrorist financing.
- All relevant employees shall receive sufficient training related to AML/CFT matters necessary for performance of their roles at the Operator.
- The Operator shall apply explicit procedures and standards of recruitment and evaluation of the employees' integrity (existing and new recruits).

The Compliance Officer: appointment and responsibilities

1. The Operator shall assign a Compliance Officer within its organization, who shall monitor compliance with Curaçao AML/CFT laws and regulations as well as with the Operator's internal policies and procedures, as referred to in art. 5g of the NOIS.
2. The Compliance Officer must hold a position within the Operator organization at least middle managerial level. The Compliance Officer may be charged with additional management responsibilities.
3. The Compliance Officer must be independent of the Casino Games Operations.
4. The Compliance Officer must be able to carry out his/her function independently and effectively, in accordance with art. 5g of the NOIS.
5. The Compliance Officer shall have timely access to customer identification data and other CDD information, transaction records, and other relevant information.
6. The Compliance Officer shall be responsible for the proper execution of the provisions in this regulation and the necessary training of the Operator personnel to be able to identify and report unusual transactions, which includes the following activities:
 - to design and implement the AML program;
 - to verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
 - to organize training sessions for the staff on various compliance-related issues;
 - to review compliance with the Operator's policy and procedures;
 - to analyze transactions and verify whether any are deemed unusual under the NORUT and hence subject to reporting to the FIU;
 - to review all internally reported unusual transactions for their completeness and accuracy with other sources;
 - to keep records of internally and externally reported unusual transactions;
 - to prepare the external report of unusual transactions;
 - to execute closer investigation of unusual or suspicious transactions;
 - to remain informed of the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements

AML Policy

and;

- to prepare periodic information on the Operator's efforts against money laundering and terrorist financing.
7. The above-mentioned responsibilities shall be included in the job description of the Compliance Officer. The job description shall be signed off on and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.
 8. The Operator shall inform the Curacao Gaming Authority and the FIU of the identity of the Compliance Officer and of any changes regarding this position.

Screening of and appropriate training plans and programs for personnel

1. The Operator ensures that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. The Operator established and adhered to proper policies and procedures in screening their employees for criminal records.
2. The Operator developed 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 regarding the Indicators for Unusual Transactions (N.G. 2015 no. 73).
3. Employees of the operator shall aware with regard to:
 - the Operator's systems and procedures for the prevention of money laundering and terrorist financing;
 - the Law and Directives issued by the competent Supervisory Authority;
 - relevant Data Protection requirements.
4. Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the Operator's policies against money laundering and terrorist financing. Each segment is trained on topics and issues that are relevant to them. Training addresses the following topics:
 - a. *New employees*

A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. They shall be made aware of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements. They must also be trained on the money laundering methods and trends in the gambling sector. They must receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.
 - b. *Dealers, cashiers and slot department personnel*

They should take a general course to understand the importance of anti-money laundering and give some basics. They need more training on how money launderers can use gambling companies to launder money. They also need to be trained in the

AML Policy

organization's procedures so they know what they should do if they recognize potential money laundering. Account opening personnel must also understand the need to verify the client's identity.

c. Audit staff

Those charged with overseeing, monitoring and testing money laundering controls should also be trained about changes in regulation, money laundering methods and enforcement, and their impact on the organization.

d. AML Compliance staff

These are the people who run the AML program. They must undergo specialized training to keep abreast of new trends or changes that impact the organization and how it manages risk.

e. Supervisors and Managers

A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

f. Senior management and board of directors

Money laundering issues and dangers should be regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that money laundering poses to the institution.

5. There is personal legal responsibility of each member of staff as regards omission to disclose information relating to money laundering and terrorist financing in accordance with the internal reporting procedures in force.
6. Staff of the Operator must be encouraged to report, without delay, matters that come to their attention in relation to transactions for which there is any suspicion that they are related to money laundering or terrorist financing. In this regard, the Operator must establish measures to ensure that staff is fully aware of their responsibilities and duties. Hence the responsibility of the Compliance Officer in cooperation with other competent departments, to prepare and implement, on an annual basis, an education and training program for the staff.
7. The training program should educate staff on the latest developments in AML/CFT and terrorist financing including the practical methods and trends used by criminals for this purpose. Training needs to be:
 - Of high quality, relevant to Operator's money laundering and terrorist financing risks, business activities and up to date with latest legal and regulatory obligations;
 - Obligatory for all relevant staff;
 - Effective; to be checked by requiring staff to pass tests and by monitoring levels of compliance with the AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
 - Ongoing, and relevant; not be limited to when staff are hired;
 - Complemented by AML/CFT information and updates that are disseminated to relevant staff.

AML Policy

8. The Board of Directors and the Senior Management must be informed of their responsibilities under the Law and this Manual and changes and developments in the legal and regulatory framework. Without this, the Board of Directors and the Senior Management will not be able to provide effective management supervision, approve policies, procedures or allocate sufficient resources for the effective prevention of money laundering and terrorist financing.
9. The Compliance Officer will evaluate the adequacy of the training provided and maintain detailed data regarding the seminars/programs.
10. The time and content of the training of the staff of different departments should be tailored to the needs of the staff and to the risk profile of the Operator. Moreover, the frequency of the training may vary depending on the amendments to the legal and/or regulatory requirements, introduction of new products, services or technologies, changes in the tasks of the staff as well as any other relevant changes.
11. It is important that all involved staff consistently implement the Operator's policy and procedures to prevent money laundering and terrorist financing and the promotion of a culture that understands the importance of the prevention of money laundering and terrorist financing, is the critical to the successful management of risks.
12. To demonstrate compliance with the aforementioned training requirements, the Operator should at all times maintain records that include:
 - details of the content of the training programs provided;
 - the names of staff who have received the training;
 - the date on which the training was delivered;
 - the results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements; and
 - an ongoing training plan.

An independent audit function to test the AML program

1. The AML compliance program must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit must be independent, thus performed by people not involved with the organization's AML compliance staff. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable.
2. These tests must include at least:
 - An evaluation of the institution's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
 - Customer's file review;
 - Compliance management;
 - Performance of transaction testing;
 - Assessment of training adequacy;
 - Assessment of compliance with applicable laws and regulations;
 - Evaluation of the system's ability to identify unusual activity;

AML Policy

- 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; and
 - An assessment of the adequacy of the record retention system.
3. The audit team should also consider whether the board was responsive to earlier audit findings.
 4. The scope of the testing and the testing results must be documented, with any deficiencies reported to Senior management and/or the Board of Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline. These corrective actions could also include enhancement of controls and procedures.

Examination by the Curacao Gaming Authority

1. The Operator shall provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the CGA in preparation of or during an examination and upon CGA request during the year.
2. The Operator shall make the following items readily available:
 - Its written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
 - Records of its Business Risk assessment;
 - The name of each Compliance Officer responsible for the Operator's overall money laundering and terrorist financing policies and procedures and his/her designated job description;
 - Records of reported unusual transactions;
 - Records of unusual transactions which required closer investigations;
 - Records of frozen accounts;
 - Schedule of the training provided to the Operator's personnel regarding money laundering, terrorist financing and proliferation of weapons;
 - The assessment report on the Operator's policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor;
 - The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.
3. The listing above is not limitative and does not exclude the Operator from providing additional information and documentation if the CGA so requests.



Appendix 1. Countries list

Prohibited countries list:	
United States of America and its territories	Myanmar (Burma)
France and its territories	Democratic People's Republic of Korea (DPRK)
Netherlands and its territories and countries that form the Kingdom of Netherlands, including Bonaire, Sint Eustatius, Saba, Aruba, Curaçao and Sint Maarten (Aruba, Bonaire, Sint - Maarten, Sint Eustatius - And Saba)	Iran
Australia and its territories	Russian Federation

The country list with increased monitoring:	
Algeria	Monaco
Angola	Mozambique
Bolivia	Namibia
Bulgaria	Nepal
Burkina Faso	Nigeria
Cameroon	South Africa
Côte d'Ivoire	South Sudan
Democratic Republic of Congo	Syria
Haiti	Venezuela
Kenya	Vietnam
Lao People's Democratic Republic	Virgin Islands (UK)
Lebanon	Yemen
Belize	Ethiopia
Dominica	Somalia
Guyana	Venezuela
Afghanistan	Cuba

