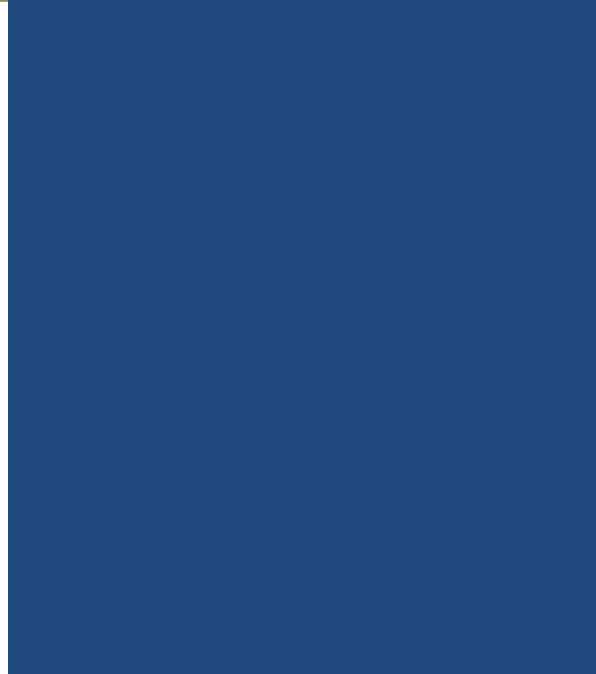




AML Policy

AML



Summary

1. Introduction	2
2. Abbreviations	2
3. Definitions	3
4. Money laundering and terrorist financing risk assessment	4
5. Customer identification and due diligence	6
6. Terrorist financing.....	19
7.Transaction monitoring.....	21
8.Policies and procedures regarding unusual transactions.....	21
9. Reporting of unusual transactions.	22
10. Responsibility for addressing risk.....	24
11. The Compliance Officer: appointment and responsibilities.....	26
12. Screening of and appropriate training plans and programs for personnel.	27
13. Examination by the Gaming Control Board.....	29

1. Introduction

1. This Manual is a guideline for **Continent Gaming N.V.**, (hereinafter called 'the Operator') 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 GCB.
6. Money Laundering is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the AML Law, so that they appear to have originated from a legitimate source. This includes all procedures to change, obscure, conceal the beneficial ownership, or audit trail of illegally obtained money or valuables.
7. Money laundering is also used to hide the link between those who finance terrorism and those who commit terrorist acts. Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts.
8. 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.

2. 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. GCB | - | Gaming Control Board |

3. Definitions

1. Compliance Officer: The officer referred to in Rule 11;
2. Crypto Asset (Virtual currency): means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by persons as a means of exchange or investment and which can be transferred, stored, and traded electronically, and it is not- fiat currency, or electronic money, or financial instruments;
3. FATF: 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;
4. 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;
5. FIU: The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT¹;
6. money laundering: The process used to conceal or disguise the nature, location, source, ownership or control of money or assets, obtained through criminal activity;
7. NOIS: National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2010, no. 40 as last amended by N.G. 2015, no. 69).
8. NORUT: National Ordinance on the Reporting of Unusual Transactions (Lands- verordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).
9. reporting code: A unique code, assigned by the FIU to each reporting entity/casino, for the purpose of reporting unusual transactions;
10. Reporting Form: The standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction;
11. Sanctions National Ordinance: The National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 1997, 336 as last amended.
12. terrorist financing: Providing or collecting funds with the knowledge that they will be used in the commission of terrorist acts;
13. transaction: an action or combination of actions by or on behalf of the client as referred to in art. 1, par. 1, sub o, of the NOIS or art. 1, par. 1, sub c, of the NORUT.

4. Money laundering and terrorist financing risk assessment

1. Risk based approach

- 1.1 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.
- 1.2 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 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.
- 1.3 The risk-based approach involves a number of steps in assessing the most effective way to manage and mitigate the money laundering and terrorist financing risks faced. These steps require the Operator to:
 - a. identify the money laundering and terrorist financing risks that are relevant to the Operator;
 - b. design and implement appropriate policies, procedures and controls to manage and mitigate these risks;
 - c. monitor the effectiveness of implemented controls and improve them if needed document what has been done, and why.
- 1.4 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.
- 1.5 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:
 - a. products, services and transactions it offers,
 - b. countries or geographic areas,
 - c. the customers it attracts, and
 - d. delivery channels it uses to service its customers.

2. Business Wide Risk Assessment

- 2.1 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:

- a. 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;
 - b. provide the written risk assessment it has prepared and the information on which it was based to the GCB on request.
- 2.2 The Business Wide Risk Assessment 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.
- 2.3 The Business Wide Risk Assessment should be signed-off at the Board level and needs to be kept up to date. Once the Business Wide Risk Assessment has been completed, the Operator should be in the position to set a "risk-appetite" which means that the Operator decides the level of risk it is prepared to accept.
- 3. Customer Risk Assessment
 - 3.1 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.
 - 3.2 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 GCB with evidence that its Customer Due Diligence measures are commensurate with the risk level.
- 4. Customer risk factors
 - 4.1 When identifying the risk associated with its customers, including its customers' beneficial owners, the Operator should consider the risks related to:
 - a. the customer's and (where appropriate) the customer's beneficial owner's business or professional activity in whatever country they are associated with;
 - b. the customer's and (where appropriate) the customer's beneficial owner's reputation in whatever country they are associated with; and
 - c. the customer's and (where appropriate) the customer's beneficial owner's nature and behavior in whatever country they are associated with.
- 5. Country/geographic risk factors
 - 5.1 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 GCB.
 - 5.2 When identifying the geographic risk associated with countries and geographical areas related to a particular customer, the Operator should consider the risk related to:

- a. the jurisdictions in which the customer and any beneficial owner are based;
 - b. the jurisdictions that are the customer's and any beneficial owner's main places of business;
 - c. the jurisdictions to which the customer and any beneficial owner have relevant personal links.
- 5.3 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. Products, services and transactions risk factors
 - 6.1 When identifying the risk associated with its products provided, services or transactions, the Operator should consider the risks related to:
 - a. the level of transparency, or opaqueness, the product, service or transaction affords;
 - b. the complexity of the product, service or transaction; and
 - c. the value or size of the product, service or transaction.
- 7. Delivery channel risk factors
 - 7.1 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:
 - a. the extent to which the business relationship is conducted on a non-face-to-face basis;
 - b. any introducers or intermediaries the Operator might use and the nature of their relationship with the Operator.

5. Customer identification and due diligence

- 1. The CDD measures must enable the Operator:
 - 1.1. to identify the customer and verify that customer's identity using reliable, independent source documents, data or information;
 - 1.2. to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner;
 - 1.3. to understand and, as appropriate, to obtain information on the purpose and intended nature of the business relationship;
 - 1.4. 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 Operator should undertake Customer Due Diligence (CDD) measures when:
 - 2.1. establishing business relations;
 - 2.2. carrying out occasional VA transactions above the monetary equivalent of US\$ 1,000; (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 US\$ 1,000);
 - 2.3. carrying out occasional fiat transactions above the monetary equivalent of US\$ 3,000; (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 US\$ 3,000).

2.4. there is a suspicion of money laundering or terrorist financing; or

2.5. the Operator has doubts about the veracity or adequacy of previously obtained customer identification data.

3. Customer Due Diligence measures consist of:

3.1. identifying the customer;

3.2. verifying the customer's identity;

3.3. 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;

3.4. assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship;

3.5. conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that:

- a. the transactions being conducted are consistent with the Operator's knowledge of the customer and the risk profile
- b. their source of funds and
- c. documents, data or information held are kept up to date.

4. Where a person claims to act on behalf of a customer, the Operator must:

- a. verify that the person is authorized to act on the customer's behalf;
- b. identify the person;
- c. 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.

5. The ways in which the Operator meets the requirements for Customer Due Diligence and the extent of the measures it takes must reflect the risk assessment it has carried out, and its assessment of the level of risk arising in any particular case. This may differ from case to case.

6. In assessing the level of risk arising in a particular case, the Operator must take account of factors including, among other things:

- a. the purpose of a customer account, transaction or business relationship;
- b. the amount deposited by a customer or the size of the transactions undertaken by the customer;
- c. the regularity and duration of the business relationship;
- d. the regularity and duration of occasional transactions.

7. Timing of Customer Due Diligence measures

7.1 The Operator must comply with the requirement of the Law to perform Customer Due

Diligence measures before the establishment of a business relationship or the carrying out of the transaction.

7.2 The Operator can do Customer Due Diligence during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is low risk of money laundering or terrorist financing. In such situations these procedures shall be completed as soon as practicable after the initial contact and before the execution of any transactions.

8. Customer relationships

8.1. Customer means a person that establishes a business relationship or performs an occasional transaction with the Operator, while a person is defined as both natural person and legal entity. Customers/person may be both individuals and legal entities.

8.2. Customer relationships for AML purposes consist of three aspects:

- a. the establishment of the business relationship with the customer, requiring verification of the customer's identity (to a reasonable degree) and completion of customer due diligence;
- b. the monitoring of customer activity (within a business relationship and risk relevant occasional transactions);
- c. the termination of the relationship with the customer.

8.3. At all stages of the relationship it is necessary to consider whether the customer is engaging in money laundering; whether there is a need to report suspicious activity; and level of risk posed to the Operator.

9. Establishment of a business relationship

9.1. 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.

9.2. In the context of the Operator, a business relationship occurs when:

- a. a customer opens an account with the Operator;
- b. a customer becomes a loyalty member (when a membership scheme is operated by the Operator);
- c. a customer applies for or is granted a credit facility at the Operator;
- d. a customer sends front money to the Operator;
- e. 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).

9.3. The list above is not exhaustive, and the Operator will need to take into consideration any other situations when circumstances otherwise arise with a customer from which it expects or it could be reasonably inferred that it expects, that the relationship with the customer will have a certain duration.

10. Occasional transactions

- 10.1. An occasional transaction is defined as any transaction other than a transaction, which takes place in a business relationship. Therefore, any transaction that is not performed during the course of a business relationship should be considered as an occasional transaction.
- 10.2. The Operator has the obligation to monitor the following occasional transactions:
 - a. Individual VA transactions with the amount of US\$ 1,000 or more, or individual fiat transactions with the amount of US\$ 3,000 or more for which the Operator has the obligation to perform Customer Due Diligence.
 - b. Linked VA transactions with the cumulative amount of US\$ 1,000 or more, or linked fiat transactions with the cumulative amount of US\$ 3,000 or more during a period of twenty-four hours. The Operator is obliged to monitor linked transactions that are individually below the US\$ 3,000 threshold but that cumulatively meet or exceed this threshold, and in such case has the obligation to perform Customer Due Diligence measures. Furthermore, in such case the Operator will need to consider whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions or days in order to circumvent the Customer Due Diligence requirements.
 - c. Occasional transactions that do not necessarily meet the requirements described under a) and b) above but are performed by customers that are gaming at the Operator on a regular basis. There may be situations where a customer performs VA transactions below the US\$ 1,000 threshold, or fiat transactions below the US\$ 3,000 threshold, but games with the Operator regularly, such that Operator needs to consider when they fall within the definition of a business relationship (i.e. having an element of duration).
- 10.3. The Operator needs to be aware that in case of customers performing individual transactions with the amount of US\$ 1,000 for VA, or US\$ 3,000 for fiat currency, or more, linked transactions with total amount of US\$ 1,000 for VA, or US\$ 3,000 for fiat currency, or more, customers performing occasional transactions on a regular basis, (as described under points a, b and c above), the business relationship is established once the element of duration is present.
- 10.4. In case that the customer plays on a regular basis, the Operator needs to determine when the criteria for the establishment of a business relationship with the customer have been met and when it needs to perform Customer Due Diligence measures.
11. The Operator should require the following documents to establish the identity:
 - 11.1. The Operator should identify the customers who are natural persons by obtaining the following information:
 - a. True name and/or names used;
 - b. Full permanent address, including postal code;

- c. Government issued document number, issuing date and country;
- d. Telephone number;
- e. E-mail address;
- f. Date and country of birth;
- g. Nationality;
- h. Details on the profession and other occupations of the customer including the name of employer/business.

11.2. 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:

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

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

- a. 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,
- b. 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.

11.3. The identification of a legal person comprises obtaining information relating to the following:

- a. The registered number, country and date of registration;
- b. The registered corporate name and trading name used;
- c. Full address of registered office;
- d. Full addresses of the Head office/principal trading offices;
- e. The telephone numbers and e-mail address;
- f. The members of the board of directors;
- g. The individuals that are duly authorized to act on behalf of the legal person;
- h. The registered shareholders that act as nominees of the beneficial owners.

11.4. The identity of a legal person shall be established through one of the documents, valid in the country of issue, referred to in art. 3, par. 2 and 3, of the NOIS:

- a. If the client is a legal person or company, the identity is established using a certified extract from the register of the Chamber of Commerce and Industry, or a similar institution, in the country of residence, or using a certificate issued by identification

document to be drawn up by the service provider. The extract or the identification document must contain at least the information to be determined by the Minister. The directors, agents and representatives of a legal person or company are identified in accordance with the first paragraph.

- b. If the client is a Curaçao legal entity under public law, the identity, without prejudice to the second paragraph, can also be established by a statement from the management. If it concerns a foreign legal entity under public law, a statement from the competent authority will suffice, without prejudice to the second paragraph.

11.5. The identity of the ultimate beneficial owner shall be established through the documents stipulated under 3.1 and 3.2.

12. The Operator shall verify the identity of the customer and the ultimate beneficial owner, using reliable, independent source documents, data or information in compliance with art. 2, par. 5, of the NOIS.

13. Verification of natural person.

13.1. Information about customer identity must then be verified through documents, data and information which come from a reliable and independent source. The acceptable method for the verification of a customer's identity is the reference to original documents which are issued by an independent and reliable source. At least one document used for verification purposes should include the customer's photo.

13.2. It is generally considered good practice and especially in high risk situations, to obtain from the customer at least one document from an authoritative source that verifies the customer's full name and address or full name and date of birth with photograph and supporting documentation that verifies their name and either date of birth or address.

13.3. The following sources may be used as the primary source of verification of customers:

- a. current passport
- b. current identity card
- c. current photo card driving license.

13.4. The above documents can be supported by a second document not used as a primary source of verification that may be:

- a. Utility bill or statement that can, on a risk basis, be verified as true by the company that issued it, commonly by confirmation of a reference number, name and address;
- b. Bank statement or passbook containing current address that can, on a risk basis, be verified as true by the company that issued it - bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth.

13.5. 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.

13.6. If documents are in a foreign language appropriate steps need to be taken to be reasonably satisfied that the documents provide factual evidence of the customer's identity.

13.7. 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.

13.8. The certifier should:

- a. sign and date the copy document (showing his name clearly in capitals underneath) and
- b. such certification should be evidenced by a written statement stating that: the document is a true copy of the original document; the document has been seen and verified by the certifier; and (where the document contains a photo) the photo is a true likeness of the customer.

14. Verification of legal entity

14.1. The verification of the identity of a legal person, comprises obtaining the following documents or documents similar to the below, depending on the jurisdiction:

- a. Memorandum and Articles of Association;
- b. Certificate of Incorporation;
- c. Certificate of Good Standing;
- d. Certificate of Registered Address;
- e. Certificate of Directors and Secretary;
- f. Certificate of Registered Shareholders in the case of private companies and public companies that are not listed in a country with disclosure and transparency requirements;
- g. In the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed;
- h. Documents and data for the verification of the identity of the persons that are authorized to act on behalf the legal person, as well as the registered shareholders and beneficial owners of the legal person.

15. Identification of beneficial owners

15.1. For the purpose of this Direction "beneficial owner" means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose

behalf a transaction or activity is being conducted and includes at least:

15.2. In the case of corporate entities:

- a. The natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements in accordance with international standards which ensure adequate transparency of ownership information.
 - i. A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person is an indication of direct ownership.
 - ii. A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), is an indication of indirect ownership.
- b. The natural person(s) who hold the position of senior managing official(s) in case that after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (a) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s).

15.3. In the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in paragraph above.

15.4. In deciding who the beneficial owner is in relation to a customer who is not a private individual, identification and verification of beneficial owners extends to legal entities that own other legal entities. The Operator should look for the natural person(s) who ultimately exercises control through ownership or through other means of the legal entity that is the customer. Control through other means may, inter alia, include the criteria of control used for preparing consolidated financial statements, such as through a shareholders' agreement, the exercise of dominant influence or the power to appoint senior management. The Operator should verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 25% in the legal person's ordinary share capital or voting rights.

15.5. There may be cases where no natural person is identifiable who ultimately owns or exerts control over a legal entity. In such exceptional cases, if all other means of identification have been exhausted, and provided there are no grounds for suspicion, senior managing official(s) are considered the beneficial owner.

15.6. The Operator should collect appropriate documents for verification of ownership structure including certificates of the registered shareholders for the companies

participating in the ownership structure of the customer, ownership charts etc. as well as appropriate information and documents for verification of identity of individual that are ultimate beneficial owners.

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

16.1. 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.

16.2. Depending on the Operator's risk assessment of the situation, information that is relevant must include as a minimum the following:

- a. The anticipated turnover/size of transactions and kind of wagering activities in which the customer is likely to engage;
- b. The origin of funds;
- c. The source and size of the customer's wealth and annual income;
- d. Regularity or duration of the relationship.

17. Ongoing due diligence:

17.1. 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.

17.2. For customers using VA information must include:

- a. IP address with an associated time stamp;
- b. geo-location data;
- c. device identifiers;
- d. VA wallet addresses;
- e. transaction hashes.

17.3. The Operator shall ensure that documents, data, and information collected through the CDD measures are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers.

18. The Operator shall develop risk profiles to determine the customer categories, which expose the Operator to higher risk.

18.1. Low-risk category includes the following customers:

- a. countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems;
- b. countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity

18.2. Medium-risk category includes the following customers:

- a. Any customer not falling under either high-risk or low-risk category.

18.3. High-risk category includes the following customers:

a. customer risk factor:

- i. business relationship is conducted in unusual circumstances;
- ii. the customer or the Beneficial owner of the customer is a PEP;
- iii. 'Customer accounts' in the name of a third person;
- iv. Customers convicted for a Predicate;
- v. Customers from countries which inadequately apply FATF's recommendations;
- vi. Other Customers that their nature entail a higher risk of ML/TF;
- vii. Any other customer determined by the Operator itself to be classified as such;

b. country risk factors:

- i. countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems;
- ii. countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
- iii. countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations;
- iv. countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operation.

19. The Operator shall conduct enhanced due diligence for high-risk customers, consistent with the risks identified.

Examples of enhanced CDD measures include:

- a. Obtaining additional information on the customer (e.g. occupation, volume and assets, information available through public databases, internet etc.) and updating more regularly the identification data of customer;
- b. Obtaining information on the source of funds or source of wealth of the customer;
- c. Obtaining the approval of senior management to commence or continue the business relationship;
- d. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

20. 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.

21. FATF- and CFATF-notifications:

21.1. The Operator shall apply enhanced due diligence measures to business relationships and transactions with persons from countries for which this is called for by the FATF and the CFATF. The type of enhanced due diligence measures applied shall be effective and proportionate to the risks.

21.2. The Operator are required to check for updates of the FATF- and CFATF notifications on a regular basis and update their Customer Due Diligence policies and – procedures accordingly to reflect these notifications.

The notifications consist of:

- a. the FATF Public Statement,
- b. the FATF Statement “Improving Global AML/CFT Compliance: On-going process”, and
- c. the CFATF Public Statement.

Note: The links to the FATF- and CFATF-notifications are published on the GCB website. The FATF-notifications are usually issued in February, June and October, and the CFATF notifications are usually issued in May/June and November/December.

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

Examples of simplifying CDD measures are:

- a. Reducing the frequency of customer identification updates;
- b. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures shall not be applied whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

22. Politically Exposed Persons (PEPs)

22.1 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.

22.2 With respect to transactions or business relationships with PEPs, 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.

22.3 In cases of business relationships or transactions with PEPs the following Enhanced Due Diligence measures must be applied:

- a. obtain Senior Management approval for establishing/continuing business relationships with such persons or performing a transaction;
- b. 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 a documentary evidence of source of wealth and source of funds;
 - c. conduct enhanced ongoing monitoring of those business relationships.
- 22.4 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.
- 22.5 Although under the definition of a PEP an individual cease to be so regarded after he has left office for 12 months, the Operator should apply a risk-based approach in determining whether or when it should cease carrying out appropriately enhanced monitoring of transactions. In cases where the PEP presents a high risk of money laundering or terrorist financing, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately decreased.
- 22.6 The Operator's policies and procedures should cover when and how customers will be checked for PEP status and how and when Senior Management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided by Senior Management.
- 22.7 There is a hierarchy of risk for individual PEPs, where some PEPs have higher relative risk and others have lower relative risk. The measures taken for particular PEPs should therefore be informed by the relative risk attributed to the PEP, including consideration of the jurisdiction from which they originate and the position they hold.
23. The Operator shall not render services to a customer:
- a. when it is known or should be assumed that the funds involved derive from corruption or misuse of public assets, without prejudice to any obligation the Operator has under criminal law or other laws or regulations; or
 - b. when the objective CDD was not met.
24. The Operator shall sustain an information program to inform their customers of the objectives of the relevant AML/CFT-legislation and inherent requirements for the Operator.
25. The Operator's internal procedures shall clearly indicate the circumstances that require customer due diligence and the required identification documents.
26. Record keeping requirements.
- 26.1 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.
- Such records shall be made readily available at the request of the Gaming Control Board.
- 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.

26.2 The Operator is obliged to record the following data in such a way that they are accessible:

- a. 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;
- b. the nature, number and date and place of issue of the document used to establish identity, except where Article 4 applies;
- c. the nature of the service.

26.3 For the required information, which the ordering institution must obtain and hold, this includes the: originator's name (i.e., the sending person's accurate (i.e. verified) full name);

- a. originator's account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA;
- b. originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth. For transmitting the geographical address of the originator, that means the address which has been verified for accuracy by the originator VASP (Virtual Assets Service Provider) as part of its KYC process ;
- c. beneficiary's name (i.e., the name of the person who is identified by the originator as the receiver of the VA transfer). This is not required to be verified by the ordering institution for accuracy, but should be reviewed for the purpose of STR (Suspicious Transaction Report) monitoring and sanction screening; and
- d. beneficiary account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA.

26.4 For the required information which the beneficiary institution must obtain from the originator institution and hold, this includes the:

- a. originator's name (i.e., the sending person's name). The beneficiary institution does not need to be verify the originator's name for accuracy, but should review it for the purpose of STR monitoring and sanction screening;
- b. originator's account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA;
- c. originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;

- d. beneficiary's name (i.e., the name of the person who is identified by the originator as the receiver of the VA transfer). The beneficiary institution must verify the beneficiary's name for accuracy, if the name of their customer has not previously verified. Thus the beneficiary institution can confirm if the beneficiary's name and account number they obtain from the ordering institution match with the beneficiary institution's verified customer data; and
 - e. beneficiary's account number where such an account is used to process the transaction. In the VA context, this could mean the "wallet address" of the VA.
- 26.5 VASPs must submit the required information to the beneficiary institution. It is vital that providers of VA transfers transmit the required originator and beneficiary information 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.
- 26.6 The Operator shall comply promptly with information requests from the GCB.
- 26.7 If doubts arise relating to the identity of the client after the Operator has accepted the client as a member and member accounts have been opened, the relationship with the client must be reexamined to determine whether it should be terminated and whether the incident must be reported to the FIU in accordance with art. 2d of the NOIS.
- 26.8 No Operator shall open or maintain an anonymous account or an account in a fictitious name.
- The Operator are required to maintain numbered accounts in such a way that full compliance can be achieved with the FATF Recommendations.
- Note: For example, The Operator should properly identify the customer in accordance with these criteria and the customer identification records should be available to the AML/CFT Compliance Officer, other appropriate staff, and competent authorities.

6. Terrorist financing

1. The Operator shall continuously monitor transactions, taking into account the characteristics including types of transactions listed in annex 1 to the FATF document entitled Guidance for Financial Institutions in Detecting Terrorist Financing. If such characteristics are identified, this could indicate funds involved in terrorist financing, so additional scrutiny is required.
2. ML and TF have important differences which must be understood in order to distinguish suspicious terrorist financial activity from ML. The most important difference involves

the origin of funds, thus TF funds are not necessarily illegally obtained, they are often clean legal funds to commit a crime. ML involves funds derived from illicit proceeds with the purpose of using them to perform legitimate activities. Also, TF uses small amounts and transactions involving unrelated parties as opposed to ML activity which involves large amounts of money.

Tracing money differs between TF and ML; in the case of TF money is used to fund TF activities by many and, in many cases, unrelated to the initiator whereas in the case of ML the funds are eventually transferred to the person (s) who initiated the proceedings.

3. According to the Law, the Operator is required to assess the TF risk inherent in their business, taking into consideration relevant factors, such as their customers and the geographical areas to which they are exposed. Amongst others, these include:

3.1 Customer risk factors:

- a. Is the customer or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures, or are they known to have close personal or professional links to persons registered on such lists?
- b. Is the customer or the beneficial owner a person who is publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity, or are they known to have close personal or professional links to such a person?
- c. Does the customer carry out transactions that are characterised by incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offences are known to be operating, that are known to be sources of TF or that are subject to international sanctions?

3.2 Countries and Geographical areas:

- a. Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities, either from official sources or from organized groups or organizations within that jurisdiction?
 - b. Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that groups committing terrorist offences are known to be operating in the country or territory?
 - c. Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?
4. The Operator are required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update their CDD- and AML/CFT policies and – procedures accordingly to reflect such amendments. Such information contains lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in (in any case):
 - a. the Consolidated United Nations Security Council Sanctions List;

- b. the EU Consolidated list of restrictive measures;
- c. the List of Financial Sanctions Targets in the UK (administered by the Office of Financial Sanctions Implementation of Her Majesty's Treasury).

Other suggested sources:

- a. the sources mentioned in annex 2 to the FATF document Guidance for Financial Institutions in Detecting Terrorist Financing; and
 - b. the listing of the Office Of Foreign Assets Control (OFAC);
 - c. other sanctions (if approved by the Management of the Operator).
5. If the Operator suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or terrorist organizations, it shall promptly report its suspicion to the FIU in accordance with art. 11 of the NORUT.

7. Transaction monitoring

1. The Operator should apply procedures and controls so as to mitigate and manage the risk of terrorist financing in relation to the transactions following the Law.
2. Especially for transaction monitoring and Customer Due Diligence, the Operator should benefit from widely available tools. Transactional analysis tools using blockchain technologies allow transactions and crypto-assets to be traced. Such tools are essential components when dealing with crypto-assets.
3. Although necessary, the use of such tools is not sufficient in itself. The Operator need to understand the risks of crypto-assets in relation to TF across the spectrum of their operations.
4. The level of transaction monitoring should be based on the Operator's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher-risk situations. The adequacy of the VASP's monitoring system and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the VASP's TF risk programme.
5. Transaction monitoring is an essential component in identifying transactions that do not fit the behavior expected from a customer's profile or that deviate from the usual pattern of transactions, thus be suspicious. The Operator should monitor transactions for any unusual activity or patterns that may be indicative of TF. This includes monitoring for transactions that are inconsistent with the customer's known business or personal activities, as well as monitoring for transactions involving high-risk countries or individuals. Specifically, the Operator should be aware of common trigger events, such as transactions involving individuals or entities on terrorism watchlists or sanctions lists or adverse media, customer information involving high-risk countries, such as IP address in regions known for terrorist activity that may indicate TF activity.

8. Policies and procedures regarding unusual transactions.

1. The Operator shall establish and maintain an AML compliance program and shall have

clear policies and procedures regarding unusual transactions.

2. The Operator must provide its staff with specific guidelines and training in recognizing and adequately documenting unusual transactions, as referred to in Rule 12.
3. To guard against money laundering and terrorist financing, the Operator must provide an audit trail for unusual transactions.
4. The Operator shall maintain the records - containing the information and documentation necessary to decide whether a transaction is deemed unusual as referred to in Rule 9 – that are related to an internal or external unusual transaction report, 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.

Such records shall be made readily available at the request of the Gaming Control Board.

9. Reporting of unusual transactions.

1. By virtue of article 11 of the NORUT, the Operator must report any unusual transaction or any intended unusual transaction to the FIU without delay. Unusual transactions shall be reported in compliance with the NORUT.
2. The Operator shall convey their policies and procedures for the reporting of unusual transactions, both internally and externally, to their personnel in an understandable way.
3. The Operator shall be responsible for the identification and reporting to the FIU of transactions that can be qualified as unusual transactions.
4. Identification of unusual transaction is the responsibility of all employees rendering services. It is the responsibility of the Compliance Officer that all employees rendering services are trained in the identification of unusual transactions and the procedures for reporting them, as referred to in Rule 12.
5. Every transaction or transaction pattern that in accordance with the NORUT is deemed unusual, shall be reported to the FIU.

The following transactions or intended transactions are deemed unusual:

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

The Operator are required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update their CDD- and AML/CFT-policies and – procedures accordingly to reflect such amendments. Sanction Decrees and Regulations and amendments are published on the GCB website.

- c. Transactions in the amount of US\$ 3,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic

or other nonphysical means. This includes but is not limited to:

- i. A cashless transaction in the amount of US\$ 3,000 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.
- ii. Accepting or releasing a deposit in the amount of US\$ 3,000 or more at the request of the client;
- iii. Sale to a client of chips in the amount of US\$ 3,000 or more.
“Chips” includes but is not limited to tokens and credits.
- iv. Pay-out of prize money in the amount of US\$ 3,000 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 in excess of the monetary equivalent of US\$ 3,000.

- d. 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.

- 6. 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 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.

Such records shall be made readily available at the request of the Gaming Control Board.

- 7. 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.
- 8. Each report about an unusual transaction will include at least the following information:
 - a. the identity of the client;
 - b. nature and number of the identification document of the client;
 - c. the nature, date, time and place of transaction;
 - d. the amount, destination and origin of the funds, or other values involved in the transaction;
 - e. the circumstances that identified the transaction as unusual.
- 9. In case of manual reporting to the FIU, the following items must be added:
 - a. Operator reporting code;
 - b. Date and time of the report;

- c. Amount of the transaction, including the currency in which it is to be executed;
 - d. In case of non-cash transactions, the bank(s) and account number(s) the client wishes to use in the transaction;
 - e. Whether or not the Operator executed the transaction;
 - f. Any other relevant facts or circumstances pertaining to the client or the proposed transaction.
10. The Compliance Officer signs the Reporting Form if it is submitted manually.
 11. The Operator will not conclude the unusual transaction if the information, necessary for the report, cannot be obtained or if the objective of the CDD measures was not met.
 12. The Operator shall report to the FIU within 48 hours the details of the transaction as recorded on the Reporting Form. The Operator can use an electronic system approved by the FIU for this purpose, or submit a paper copy of the Reporting Form. Submission of paper forms shall not be done by fax for the purpose of data security. In either case, the Operator will retain a copy of the Reporting Form for its own records, which are available to GCB Agents upon request.
 13. Submission of Reporting Forms will be confirmed in a confirmation letter from the Operator to the FIU, which references only the transaction numbers of the submitted Reporting Forms.
 14. The FIU shall confirm receipt of confirmation letters by means of a stamped, signed and dated return of the confirmation letter. This letter confirms receipt of the corresponding Reporting Forms and serves as indemnification in a civil or criminal procedure. The Operator shall file such letter with the copy of the original Reporting Form.

10. Responsibility for addressing risk

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:
 - a. 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.

- b. 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.
- c. 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.
- d. 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.
- e. 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.
- f. The Compliance Officer should have sufficient resources to undertake their duties. This includes but is not limited to, competent staff, technological and equipment, and access to responsible executive(s) for the effective discharge of their duties. The Compliance Officer and any other person assigned with the duty of implementing or reviewing the program and procedures for the prevention of money laundering and terrorist financing should have complete and timely access to all relevant data and information concerning customers' identity, transactions and other information maintained by the Operator so as to be effective in their duties.
- g. 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:
 - I. 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,
 - II. The use of new or developing technologies relating changes in existing products or their delivery, and
 - III. Possible changes in the business model of the Operator.Risk assessments should take place prior to the launch of the new/ changed products, business practices or the use of new or developing technologies.
- h. 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.
- i. 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.

- j. 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.
- k. 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.
- l. 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 GCB 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.
- m. All employees should be 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.
- n. 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.
- o. 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.
- p. All relevant employees shall receive sufficient training related to AML/CFT matters necessary for performance of their roles at the Operator.
- q. The Operator shall apply explicit procedures and standards of recruitment and evaluation of the employees' integrity (existing and new recruits).

11. 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:
- a. to organize training sessions for the staff on various compliance-related issues;
 - b. to review compliance with the Operator's policy and procedures;
 - c. to analyze transactions and verify whether any are deemed unusual under the NORUT and hence subject to reporting to the FIU;
 - d. to review all internally reported unusual transactions for their completeness and accuracy with other sources;
 - e. to keep records of internally and externally reported unusual transactions;
 - f. to prepare the external report of unusual transactions;
 - g. to execute closer investigation of unusual or suspicious transactions;
 - h. to remain informed of the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements and;
 - i. 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 Gaming Control Board and the FIU of the identity of the Compliance Officer and of any changes regarding this position.

12. Screening of and appropriate training plans and programs for personnel.

1. The Operator shall ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. The Operator shall establish and adhere to proper policies and procedures in screening their employees for criminal records.
2. The Operator shall develop training programs and provide training to all personnel who perform transactions as referred to in the NOIS and the NORUT.
3. Training includes setting out rules of conduct governing employees' behavior and their ongoing education to create awareness of the Operator's policy against money laundering and terrorist financing.
4. Employees of the operator shall aware with regard to:
 - a. the Operator's systems and procedures for the prevention of money laundering and terrorist financing;
 - b. the Law and Directives issued by the competent Supervisory Authority;
 - c. relevant Data Protection requirements.
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:
 - a. 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;
 - b. Obligatory for all relevant staff;
 - c. Tailored to the particular roles of the staff; the training program should have a different structure for new staff, front-line staff, compliance staff, staff moving from one department to another etc.;
 - d. 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;
 - e. Ongoing, and relevant; not be limited to when staff are hired;
 - f. Complemented by AML/CFT information and updates that are disseminated to relevant staff.
 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:
 - a. details of the content of the training programs provided;

- b. the names of staff who have received the training;
- c. the date on which the training was delivered;
- d. the results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements; and
- e. an ongoing training plan.

13. Examination by the Gaming Control Board.

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 GCB in preparation of or during an examination and upon GCB request during the year.
2. The Operator shall make the following items readily available:
 - a. its written and approved policy and procedures on money laundering and terrorist financing prevention;
 - b. the name of the Compliance Officer responsible for the Operator's overall money laundering and terrorist financing deterrence and detection procedures and her/his designated job description;
 - c. records of reported unusual transactions;
 - d. records on unusual transactions which required closer investigations;
 - e. the completed source of funds declaration;
 - f. schedule of the training provided to the Operator's personnel regarding money laundering and terrorist financing;
 - g. the assessment report on the Operator's policies and procedures on money laundering and terrorist financing by the internal audit department or the Operator's external auditor;
 - h. required copies of identification documents.
3. The listing above is not limitative and does not exclude the Operator from providing additional information and documentation if the GCB so requests.