

OLYMPUS HOLDINGS N.V.

INTERNAL PROCEDURES MANUAL

The manual is property of Olympus Holdings N.V. The reproduction in whole or in part in any way including the reproduction in summary form, the reissue in a different manner and any changes in the original manual or any translated version is strictly forbidden and is only allowed with the prior written consent of Olympus Holdings N.V.

INDEX

Table of Contents

PART I

1.	INTRODUCTION	5
2.	LEGAL FRAMEWORK.....	6
3.	SERVICES	7
4.	ORGANISATIONAL STRUCTURE	8
5.	OBLIGATIONS WHEN PROVIDING ONLINE SERVICES TO CLIENTS	9
6.	CAPITAL REQUIREMENTS	9
1.	BOARD OF DIRECTORS AND SENIOR MANAGEMENT RESPONSIBILITIES POLICY	9
1.1	Responsibilities of Board of Directors.....	9
1.1.1	Board of Directors Meetings	10
1.2	Senior Management	10
1.2.1	Responsibilities of Senior Management.....	10
2.	COMPLAINTS OR GRIEVANCES POLICY.....	11
2.1	Complaint or grievance handling.....	11
2.2	Record-keeping of complaints or grievances received	11
3.	RECRUITMENT OF PERSONS POLICY	11
3.1	Policy	11
3.2	Qualifications	11
3.3	Employee Screening.....	12
3.4	Staff training, supervision, education	12
4.	CONFLICTS OF INTEREST POLICY	13
4.1	Introduction	13
4.2	Scope.....	13
4.3	General Identification of Conflicts of Interest	13
4.3.1	General Principles	13
4.3.2	Criteria and Circumstances	14
4.3.3	Non-Exhausting list of Circumstances of Conflicts of Interest:	14
4.3.4	Personal Transactions of Employees.....	15
4.4	Management of Conflicts of Interest.....	15
4.4.1	Independence	15
4.4.2	Specific Identification of Conflict of Interest and Measures for their Management	16
4.4.3	Disclosure of Conflict of Interest	16
4.4.4	Record Keeping	16
4.4.5	Enforcement and Review of the Policy	16
4.5	Client's Consent	17
5.	RECORD KEEPING POLICY	17

6.	BUSINESS CONTINUITY POLICY	19
6.1	Policy	19
6.2	Continuity of IT systems.....	19
7.	OUTSOURCING POLICY	19
7.1	Outsourcing and Company's responsibility.....	19
8.	PRIVACY POLICY.....	20
8.1	Our Commitment	20
8.2	Collection of Information	20
8.3	Use of the Information.....	20
8.4	Contacting clients	20
8.5	Disclosure of Information	20
8.6	Safeguard Measures	21
9	COMPLIANCE POLICY	22
9.1	Policy.....	22
9.2	Reporting obligations:.....	22
10	AML POLICY	24
10.1	Duty to cooperate for prevention of Money Laundering and other criminal activities	24
10.1.1	The role of the Board	24
10.1.2	The role of the Senior Management	25
10.2	CUSTOMER ACCEPTANCE POLICY	26
10.3	Recognition and reporting of suspicious transactions.....	26
10.4	Customer Due Diligence	27
10.4.1	KYC Documentation for natural persons.....	30
10.4.2	KYC Documentation for Executorship Accounts	
10.5	Customers' Profile Policy	31
10.6	Risk based approach	32
10.7	Simplified customer due diligence	33
10.8	Enhanced customer due diligence	33
10.9	Other obligations of the Company.....	33
10.10	Reporting of suspicious transactions by the Company	34
10.11	Company to appoint a compliance officer and establish procedures, etc.....	35
10.11.1	Appointment of MLRO	36
10.11.2	Duties of MLRO	37
10.11.3	Internal audit.....	38
1.	FINANCE AND ACCOUNTING DEPARTMENT	39
1.1	Accounts payable monitoring	39
1.2	Accounting Records Maintenance	39
1.3	Accurate records	39
1.4	Retention of records	39
2.	BACK OFFICE / ACCOUNT OPENING DEPARTMENT.....	40

Internal Procedures Manual

2.1 Open a new client account	40
2.2 Procedures for client identification	40
2.3 Payment on an account	40
2.4 Individual clients	41
2.6 Accounts maintenance.....	41
2.7 Marketing Communication	41
2.7.2 Withdrawal and Refund Policy.....	42
3. INFORMATION TECHNOLOGY DEPARTMENT	43
3.1 Procedures:	43

1. INTRODUCTION

The purpose of the Olympus Holdings Ltd (hereinafter the “**Company**”) Internal Operations Manual is to lay down the procedures and the control systems based on which the Company operates. The Internal Operations Manual (hereinafter the “**Manual**”) contains instructions and rules for the execution of the work and the obligations of the management and personnel of the Company, so that, to the best of the efforts of the Company, no omissions and ambiguities exist as to the work content and professional conduct towards the Clients of the Company.

In addition, the Manual comprises processes which procure for:

- (a) the establishment of standards and specifications of quality levels for all the Company’s operations, aiming to achieve equal levels of quality in all the services provided by the management and employees of the Company.
- (b) the availability of the procedures and rules for the operation of the Company, both to the people in charge of the performance of the operations of the Company, as well as to the employees responsible for auditing the operations.

The Manual has been prepared so that it complies with, and applies, the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, PB 1993, no. 63) (“**NOOGH**”) (“**Laws and Regulations**”).

The Manual has been prepared by the Board of Directors of the Company in accordance with the Laws and Regulations. The Board of Directors bears the responsibility for the adequacy of the processes and the control safeguards applied. It is also the responsibility of the Board of Directors to review and update the Manual as may be required from time to time, and for such updates to be fully in line with the amendments in the Laws and Regulations.

A breach or non-compliance with the Provisions / Obligations to the Laws and Regulations as well as the AML/CFT Policy of the Manual may result in the revocation of the Company’s license.

2. LEGAL FRAMEWORK

The Company holds Securities Intermediary License (“**License**”) pursuant to the National Ordinance on the Supervision of Securities Brokers and Asset Management Companies, as amended.

As an entity incorporated in Curaçao and licensed by the Curaçao Gaming Control Board (“GCB”), the Company will have to comply with the existing rules and regulations of Curaçao, and any subsequent rules and regulations superseding the existing ones. These include but are not limited to the following:

- (a) the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, PB 1993, no. 63) (NOOGH)
- (b) the National Ordinance on reporting of Unusual Transactions (NORUT)
- (c) the National Ordinance on Identification when Rendering Financial Services (NOIS)
- (D) the Sanctions National Ordinance (Sanctielandsverordening, PB 2014, no. 55, GT) (SNO)
- (e) National Ordinance on identification when rendering services (LID)
- (f) the National Ordinance on the reporting of unusual transactions (LMOT)
- (g) National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282)
- (h) the National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283)
- (i) LB no. 19/0283 Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector
Appointment of the GCB as the AML/CFT supervisor for the LMOT for the gaming industry.
- (j) PB 2020, 157 | Landsbesluit inzake regels voor melding ongebruikelijke transacties (Landsbesluit goAML meldportaal)
Rules for reporting unusual transactions.
- (k) PB 2015, 73 | Regeling indicatoren ongebruikelijke transacties
Indicators for recognizing unusual transaction.

The above shall be collectively termed as “**Laws and Regulations**”.

3. SERVICES

It is proposed that, once the Online Gaming License has been granted, the Company shall conduct its business as per governance ruled Conditions of the Curacao Online Gaming License and provide the below detailed functions and activities. The Company shall comply with all policies, procedures, regulations, guidelines and directives that may be set by the GCB with regard to the licensed games of chance, and the way in which these should be organized, including policies, procedures, regulations, guidelines and directives pursuant to the NORUT and NOIS.

The Company plans to combine range of casino games offered on its platform, including video slots, blackjack, roulette, poker, and other popular games, offering of diverse remote games of chance services to its clients.

The Company shall not on-board Clients from countries that are on the Financial Action Task Force (FATF) that have strategic deficiencies in their standards of AML.

The services will be provided to clients through an online gaming platform which will be incorporated on the website to be operated by the Company. The Company shall have a gaming Account opened in the name of each client in order to facilitate gaming activity.

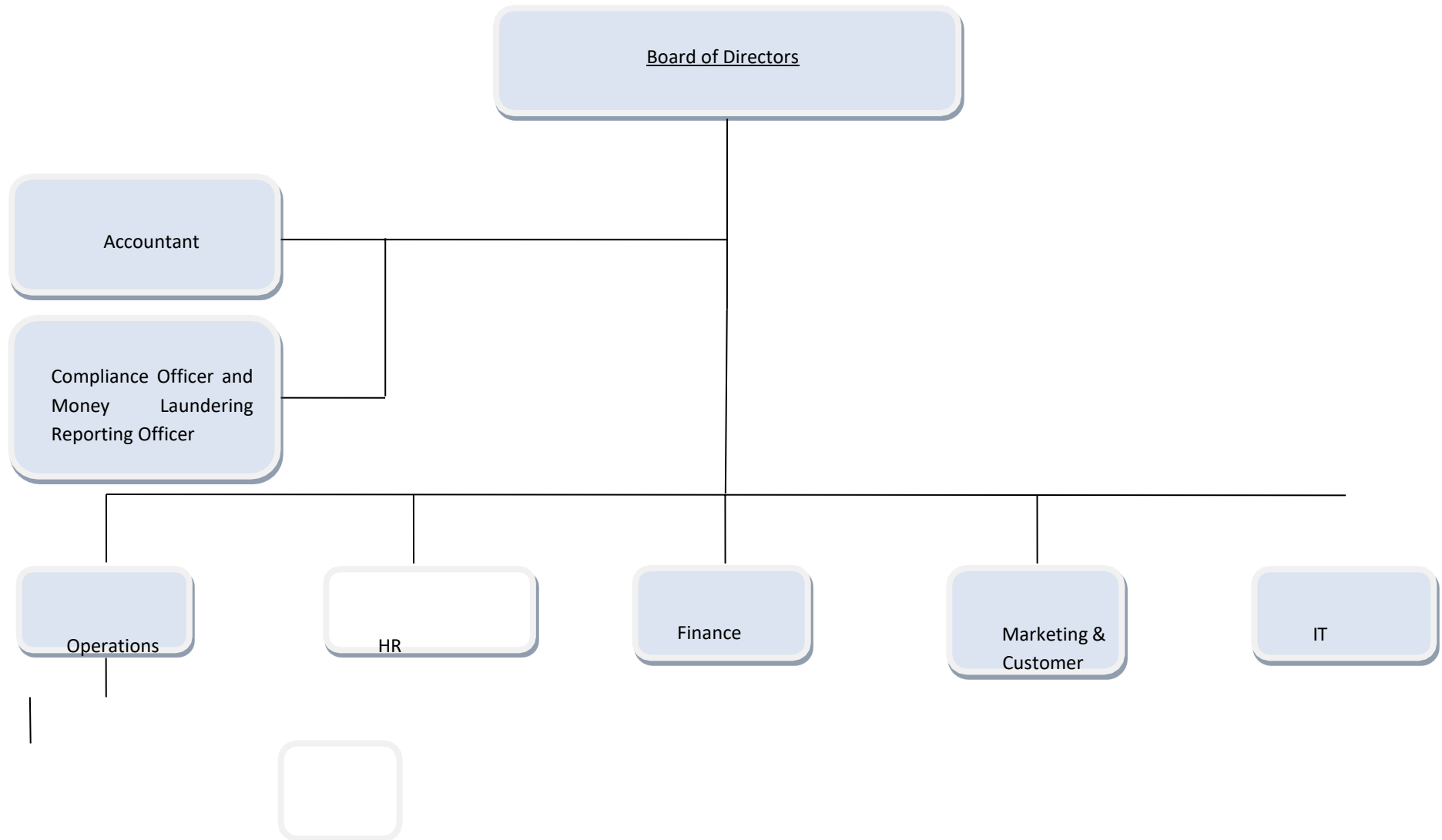
Casino Offerings: Video Slots, Online Casino: Our platform, based on the “Oryx” platform, owned by the BGRAGG Gaming Group, with the best of breed game providers such as playson, Betsoft, Red Tiger, Wazdamn, Quick spin, Microgaming, Ezugi, Boongo, and Vivo Gaming will boast an extensive array of both classic and contemporary casino games, encompassing slots, blackjack, roulette, poker, and beyond. Collaborations with these premier game developers will ensure a diverse and top-tier gaming milieu for our clientele.

Sports Betting: In the future, the Company may contemplate the incorporation of a comprehensive sports betting platform, covering prominent sporting events globally. Patrons will gain access to a spectrum of betting options, live streaming services, and real-time updates, thereby enriching their sports betting involvement

Mobile App: We shall forge ahead with the development of an intuitive mobile application, compatible with both iOS and Android platforms, enabling users to seamlessly access our platform and relish their preferred games and betting opportunities on the move.

Customer Support: The Company pledges to deliver round-the-clock customer support, catering to users' queries, technical glitches, or concerns. Our adept team of professionals will ensure swift and effective resolution of customer issues, thereby augmenting overall user contentment.

4. ORGANISATIONAL STRUCTURE



5. OBLIGATIONS WHEN PROVIDING ONLINE GAMBLING SERVICES TO CLIENTS

The Company shall, when providing online gambling services to clients, act honestly, fairly and professionally in accordance with the best interests of its clients and comply, in particular, with the following principles:

- (a) All information, including marketing communications, addressed by the Company to its clients or potential clients shall be fair, clear and not misleading; marketing communications must be clearly identifiable as such;
- (b) The Company must provide to its clients or potential clients appropriate information in a comprehensible form about:
 - i) The Company and its services;
 - ii) Type of games of chance ; this should include appropriate guidance on and warnings of the risks associated with gambling in those games of chance;
 - iii) The Gambling platform,
 - iv) costs and associated charges, if any, so that they are reasonably able to understand the nature and risks of the online gambling service and of the specific type of game of chance that are being offered and, consequently, to take decisions on an informed basis. This information may be provided in a standardized format.
- (c) The Company must establish a record that includes the document or documents agreed between the Company and the client that set out the rights and obligations of the parties, and the other terms on which the Company will provide services to the client; the rights and duties of the parties to the contract may be incorporated by reference to other documents or legal texts.
- (d) The Company must provide all of its customers with monthly statements with the following specified information:
 - i) the amount due, if at all, to such customers; and
- (e) the fact that such funds are payable on demand of the customer. The Company is required to fully disclose to customers the charges for services performed by registered firms in connection with securities transactions and shall not be discriminatory between customers.

6. CAPITAL REQUIREMENTS

The Company shall at all times ensure that the Company has sufficient capital to guarantee the sound and proper continuance of the company's operations and performance of its obligations.

PART II GENERAL PROCEDURES/POLICIES

1. BOARD OF DIRECTORS AND SENIOR MANAGEMENT RESPONSIBILITIES POLICY

1.1 Responsibilities of Board of Directors

The Board shall have the following responsibilities:

- (a) ensuring that the Company complies with its obligations under the Laws and Regulations, including undertaking risk assessment of the business and its clients and review of the risk assessment systems on a yearly basis to ensure an effective system is in place and swift action to be taken to remedy any

identified deficiencies.

- (b) assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the obligations under the legal framework, and to take appropriate measures to address any deficiencies.
- (c) ensure that it shall receive on a frequent basis, and at least half yearly, written reports regarding AML/CFT indicating, in particular, whether the appropriate remedial measures have been taken in the event of any deficiencies, as and if applicable.
- (d) monitoring of the internal control mechanisms of the Company to enable prevention of activities outside the scope and strategy of the Company and the prevention of any unlawful transactions, the identification of risks, and the timely and adequately flow of information.
- (e) ensure adequate resources are given to the CO/MLRO to enable the standards as per prevailing regulations to be adequately implemented and periodically monitored and tested.
- (f) ensure procedures are established and maintained which allow the CO/MLRO and the DMLRO to have access to all relevant information, which may be of assistance to them in considering STRs.
- (g) Encourage and facilitate disclosure to the Financial Intelligence Unit ("FIU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or TF, including attempted ML and/or TF.
- (h) maintain records for the prescribed periods of time
- (i) The Company shall adhere to the Corporate Governance principles enunciated in the Laws and Regulations or any new codes issued subsequently.
- (j) The Board shall pass a resolution for selecting a service provider or individual for outsourcing.

1.1.1 Board of Directors Meetings

The Board shall meet at least annually. During these meetings, review of (1) the Company's performance in the preceding year and prospects for the ensuing year; (2) the general strategy of the Company and (3) AML/CFT reports and risk assessments shall be included in the agenda, among others.

The Company shall maintain in their offices such board meeting minute books and general meeting minute books as are required by law.

1.2 Senior Management

The Senior Management is appointed by the Board of Directors. The members of the Senior Management will be the persons who effectively direct the business of the Company. As such, they will be addressing and resolving the day-to-day operational issues of the Company.

1.2.1 Responsibilities of Senior Management

The Senior Management shall be responsible for the following:

- a) ensure that the Company complies with its legal obligations and review the effectiveness of policies, arrangements and procedures followed by the Company in relation to the Company's obligations under the legal framework.
- b) Encourage and facilitate disclosure to the Financial Intelligence Unit ("FIU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or TF, including attempted ML and/or TF.
- c) maintain records for the prescribed periods of time.
- d) Procedural Reviews. Management should review at regular intervals the operational efficiency and quality of services provided to clients by their respective teams. This should include an evaluation of workflows, division of work, allocation of responsibilities etc.
- e) reviews the activities of each of the Company's departments to address any deficiencies identified.

- f) Present to the Board of Directors issues that need to be discussed and resolved.

2. COMPLAINTS OR GRIEVANCES POLICY

2.1 Complaint or grievance handling

The Company shall establish, implement and maintain effective and transparent procedures for the reasonable and prompt handling of complaints or grievances received from retail or potential retail clients, and to keep a record of each complaint or grievance and the measures taken for the complaint's resolution.

Clients' complaints or grievances are initially handled by the Back Office/Account Opening Department. However, the final settlement of non-trivial complaints or grievances needs to be approved by Senior Management.

The Company shall promptly address any complaints from its customers and do everything possible to satisfy them so as to avoid any damage to the reputation of Curaçao as a well-regulated jurisdiction.

A dedicated email shall be setup to receive any client complaints. Moreover, there shall also be an option to submit a complaint on the Company's website.

2.2 Record-keeping of complaints or grievances received

The Company shall maintain a Complaint Register which shall contain details of the complaint/grievances including action taken for a minimum period of seven years. The responsible department shall be the Back Office / Account Opening Department.

3. RECRUITMENT OF PERSONS POLICY

3.1 Policy

The Company shall establish, implement and maintain a Recruitment of Persons Policy. The Company will recruit its employees by implementing the relevant procedures set out below.

The Company will keep records of all information, documents and supporting documents received during the recruitment process.

3.2 Qualifications

Persons employed by the Company will meet the following criteria:

a. Good repute

Persons employed by the Company will have integrity, morals and credibility. For this purpose, the Company will request the submission of the following, which will be kept in the Company's records:

- (a) Copy of passport or ID card.
- (b) Certificate or copy of certificate of non-bankruptcy, certifying that the person is not bankrupt.
- (c) Certificate or a copy of criminal record certificate from the competent authorities of the country of residence of the person for the last five years, attesting that the person has no criminal record.
- (d) Questionnaire prepared by the Company and completed and signed by the person employed.
- (e) Constituent/s letter/s from people who know very well the person in questions i.e. letter from previous employers.

b. Skills, knowledge and expertise

Persons employed by the Company will hold academic and/or have professional qualifications and professional experience relevant to the responsibilities assigned to them. For this purpose, the Company will request the submission of the following, which will be kept in the Company's records:

- (a) Copies of academic degrees or diplomas, or/and professional qualifications.
- (b) Certificates from previous employers showing that the person has experience relevant to the assigned responsibilities.

3.3 Employee Screening

The Company shall implement screening procedures so that high standards are maintained when hiring employees.

In order to ensure that employees, depending on their role, are of the required standard of competence, including meeting the GCB standards, the Company must give consideration to the following prior to, or at the time of, recruitment:

- obtaining and confirming details of employment history, qualifications and professional memberships.
- obtaining and confirming appropriate references.
- Obtaining and confirming details of any disciplinary action taken against the employee by the previous employer(s).
- obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee.
- obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record.
- Undertaking checks using appropriate risk management systems and Google search on the employee.
- screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.
- The Company should also carry out periodic ongoing of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

3.4 Staff training, supervision, education

- (a) The Company shall ensure that their relevant staff are adequately trained and supervised to ensure proper compliance with the legal framework and any other relevant laws, regulations and procedures, as the case may be.
- (b) The Company and its relevant personnel shall familiarize themselves with the risks of inadvertent involvement in money laundering or other criminal activity and, at induction, and routinely thereafter, measures should be taken to ensure that they are aware of all relevant legislative requirements and any relevant guidelines and procedures relating to the recognition and avoidance of such criminal activities.
- (c) The Company shall encourage vigilance amongst their staff to avoid involvement in money laundering or other criminal activity not only where such staff give support services or manage direct contact with clients but also where appropriate, among clerical, secretarial or administrative staff and, in particular, in accounting departments.
- (d) The Company shall ensure staff compliance with the legal framework and relevant guidelines; and internal policies shall be monitored on a regular basis including compliance with procedures for establishing and maintaining appropriate records.
- (e) The Company shall ensure that its relevant staff at the commencement of employment are made aware of what constitutes money laundering and their potential personal liability under the money laundering legislation, and due attention shall be given in training to combat and prevent money laundering.
- (f) More specifically the contents of training shall include the following:
 - i) Awareness and brief of the Laws and Regulations.

- ii) The Company's policies, procedures and controls manual for AML and CFT (copies should be provided to staff or link to where these are saved electronically) including procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.
- iii) the Company's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships.
- iv) the identity and responsibilities of the MLRO, CO and Deputy MLRO.
- v) how to competently analyze information and documentation, so as to enable the formation of an opinion on whether the transactions and actions may be linked to ML or TF.
- vi) the identification and examination of unusual transactions or activity outside of that expected for a customer.
- vii) the nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist-related.
- viii) the vulnerabilities of the Company to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs.
- ix) UN, EU and other sanctions and the Company's controls to identify and handle natural persons, legal persons and other entities subject to sanction.
- x) new developments in ML and TF, including information on current techniques, methods, trends and typologies.
- xi) those aspects of the Company's business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by the Company, including any new products, services or delivery channels and any technological developments.
- xii) detail procedures that need to be followed if any links to ML or TF have been identified.
- xiii) the requirements for the internal and external disclosing of suspicion.
- xiv) dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers.
- xv) the implications of non-compliance by employees to requirements of the Manual other internal guidelines and policies and the Laws and Regulations.
- xvi) the criminal and regulatory sanctions in place, both in respect of the liability of the Company and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the Company.

The list included above is non-exhaustive and there may be other areas the Company may deem appropriate to include, based on the business of the Company and the conclusions of its business risk assessments.

4. CONFLICTS OF INTEREST POLICY

4.1 Introduction

The Company is committed to act honestly, fairly and professionally and in the best interests of its Clients and to comply, in particular, with the principles set out in the above Laws and Regulations when providing online gaming services and ancillary services related to such online gaming services.

4.2 Scope

The purpose of this policy is to set out the Company's approach in identifying and managing conflicts of interest which may arise during the course of its normal business activities. In addition, this policy identifies circumstances which may give rise to a conflict of interest. The Policy applies to all its directors, employees, any persons directly or indirectly linked to the Company (hereinafter called "Related Persons") and refers to all interactions with all Clients.

4.3 General Identification of Conflicts of Interest

4.3.1 General Principles

When the Company deals/transacts with the Client, the Company (or an associate or any other person connected with the Company) may have an interest, relationship or arrangement in relation to the Transaction concerned or

that it conflicts with the Client's interest. The Company hereby identifies and discloses a range of situations and circumstances which may give rise to a conflict of interest and potentially, but not necessarily, be detrimental to the interests of one or more Clients. The Company shall take all appropriate steps to identify conflicts of interest situations between the Company and its Related Persons, the Company and its Clients or between its Clients during the course of the provision of online gaming services. The Company's Policy, in general:

- identifies circumstances which may give rise to conflicts of interest entailing a material risk of damage to the interest of the Client.
- specifies appropriate mechanisms and systems to manage the potential conflicts.
- maintains systems designed to prevent damage to our clients' interests through identified conflicts.

The affected parties if conflict of interest arises can be the Company, its employees or its clients. More specifically, a conflict of interest may arise, between the following parties:

1. Between the client and the Company.
2. Between two clients of the Company.
3. Between the Company and its employees.
4. Between a client of the Company and an employee/ manager of the Company.
5. Between Company's Departments.

4.3.2. Criteria and Circumstances

For the purposes of identifying the types of conflicts of interest that may arise in the course of providing online gambling services whose existence may damage the interest of a Client, the Company takes into account, whether the Company or a relevant person, is in any of the following situations, whether as a result of providing online gambling services:

- The Company or a Related Person is likely to make a financial gain or avoid a financial loss at the expense of a Client.
- The Company or a Related Person receives or will receive from a person other than the Client an inducement in relation to a service provided to the Client, in the form of monies, goods or services, other than the standard commission or fee for that service.
- The Company or a Related Person has an interest in the outcome of a service provided to the Client or of a transaction carried out for the Client, which is distinct from the Client's interest in that outcome.
- The Company or a Related Person has a financial or other incentive to favor the interest of another Client or group of Clients over the interests of the Client.
- The Company or a Related Person carries on the same business as the Client.

4.3.3. Non-Exhausting list of Circumstances of Conflicts of Interest:

While it is not feasible to define precisely or create an exhaustive list of all relevant conflicts of interest that may arise, as per the current nature, scale and complexity of the Company's business, the following list includes circumstances which constitute or may give rise to a conflict of interest entailing a material risk of damage to the interests of one or more Clients, as a result of providing online gaming services:

- (a) The possible use of confidential information derived from the different departments of the company.
- (b) the Company is likely to make a financial gain, or avoid a financial loss, at the expense of the client.
- (c) the Company may receive or pay inducements to or from third parties due to the referral of new Clients or Clients' wagering.
- (d) Any game of chance information, training and discussions as regards possible game of chance should not be construed as manipulation of the game or its outcome. It is the client responsibility to perform its own independent discretion before entering into any wagering standing.

Company employees are required to comply with a policy of independence and to disregard any such material interest or conflict of interest while offering services to the Client.

4.3.4. Personal wagering of Employees

All employees of the Company that are involved in activities that the Company is authorized to provide must be aware of the restrictions on personal wagering detailed below. This section also includes personal wagering which may be performed by persons who are employed by companies which perform an outsourced activity to the Company, if any. In case where any prohibited personal wagering are entered into, the Company must be notified promptly.

Employees of the Company that are involved in the provision of online gaming services or other activities must **not** enter into the personal wagering that which will cause the following:

- enter into a wagering prohibited under the Laws and Regulations.
- misuse or cause improper disclosure of confidential information.
- enter in a wagering that is likely to conflict with any obligations of the Company, or the employee, that are stated under the Laws and Regulations.

Where the employee has come into contact with information which is not publicly available to clients or cannot readily be inferred from information that is so available, the employees must not act or undertake personal transactions or wager personally or on behalf of any other person.

The employees should also refrain from disclosing any opinion other than in the normal course of business, if the person who is given the opinion is likely to enter into a transaction which is contrary to the above. The employee should further not provide an advice or provide to anyone any information, other than in the proper course of his/her employment, especially if it is clear that the person who is receiving such information will advise another party who might acquire or dispose of wagering games of chance to which that information relates.

Any client's wagers that have been relayed to any employees of the Company must not be disclosed to another party. An employee of the Company who has knowledge of a potential client's order must not carry out a personal transaction that is the same as the client order, if this will cause a conflict of interest.

4.4 Management of Conflicts of Interest

4.4.1 Independence

The following measures have been adopted by the Company for ensuring the requisite degree of independence (list is not exhaustive):

- (a)The Company undertakes ongoing monitoring of business activities to ensure that internal controls are appropriate.
- (b)The Company undertakes effective procedures to prevent or control the exchange of information between Related Persons engaged in activities involving a risk of a conflict of interest where the exchange of that information may harm the interests of one or more Clients.
- (c)The separate supervision of Related Persons whose principal functions involve providing services to Clients whose interests may conflict, or who otherwise represent different interests that may conflict, including those of the Company.
- (d)Measures to prevent or limit any person from exercising inappropriate influence over the way in which the Related Person carries out online gambling services.
- (e)Measures to prevent or control the simultaneous or sequential involvement of a Related Person in separate online gambling services where such involvement may impair the proper management of conflicts of interest.
- (f)A policy designed to limit the conflict of interest arising from the giving and receiving of inducements.
- (g)Chinese walls restricting the flow of confidential and inside information within the Company, and physical separation of departments.
- (h)Procedures governing access to electronic data.
- (i)Segregation of duties that may give rise to conflicts of interest if carried on by the same individual.
- (j)Personal account dealing requirements applicable to Related Persons in relation to their own online gambling activities.
- (k)Establishment of in-house Compliance Department to monitor and report on the above to the Company's Board of Directors.

- (l) Prohibition on officers and employees of the Company having external business interests conflicting with the interests of the Company without the prior approval of the Company's board of directors.
- (m) A "need to know" policy governing the dissemination of confidential or inside information within the Company.
- (n) Appointment of Internal Auditor to ensure that appropriate systems and controls are maintained and report to the Company's Board of Directors.
- (o) Establishment of the "four-eyes" principle in supervising the Company's activities.

4.4.2. Specific Identification of Conflict of Interest and Measures for their Management

The Company is constantly conducting an in-depth analysis of its business and organizational arrangements including best execution arrangements, inducement practices, remuneration practices and online gaming research/marketing communication procedures, to ensure that all likely conflict of interest situations are identified regardless of materiality.

4.4.3 Disclosure of Conflict of Interest

The Company must adequately consider how to manage all conflicts of interest before resorting to disclosure. This will be a last resort after all appropriate steps have been taken.

When the measures taken by the Company to manage conflicts of interest are not sufficient to ensure with reasonable confidence that risks of damage to clients' interest will be prevented, the Company proceeds with the disclosure of conflicts of interest to the client. Prior to carrying out a transaction or before providing an online gambling services to a client, the Company must disclose any actual or potential conflict of interest to the client. The disclosure will be made in sufficient time and in a durable manner and shall include sufficient detail, taking into account the nature of the client, to enable him to take an informed decision with respect to the online gambling services in the context of which the conflict of interest may arise. Clients will be given the opportunity to decide on whether or not to continue their relationship with the Company due to the conflict disclosed, without being unreasonably prohibited to do so.

4.4.4 Record Keeping

The following documentation shall be maintained for at least 10 (ten) years.

- this policy, any functional variations if applicable.
- the Conflicts Log and the Conflicts Identification and Management Map.
- rules, procedures and processes.
- training material and training records.
- Conflicts of Interest Notification Forms.
- details of any review work carried out (including any decisions made on conflicts management).
- any other documentation used to demonstrate the management of conflicts of interest.

4.4.5 Enforcement and Review of the Policy

The Company's Chief Executive Officer is responsible for clearly allocating responsibility and delegating authority to accountable individuals to ensure that those involved are aware of their involvement and that the Conflict Officer has a sufficient level of authority and independence in order to carry out their responsibilities effectively. The Company's Senior Management is required to:

- fully engage in the implementation of policies, procedures and arrangements for the identification, management and ongoing monitoring of conflicts of interest; adopt a holistic view to ensure the identification of potential and emerging conflicts within and across business lines and to ensure that informed judgments are made with respect to materiality.
- raise awareness and ensure compliance of relevant individuals by ensuring: regular training (including to contractors and third-party service providers' staff) both at induction and in the form of refresher training; the clear communication of policies, procedures and expectations; that awareness of conflicts procedures forms part of the performance review/appraisal process, and that the best practice is shared throughout the Company.

- sponsor robust systems and controls and effective regular reviews to ensure that strategies and controls used to manage and mitigate risks remain appropriate and effective and that appropriate warnings and disclosures are issued to clients where necessary.
- utilize management information to remain sufficiently up-to-date and informed.
- support an independent review of the processes and procedures in place.

Individuals are required to identify new conflicts of interest arising out of the activities/ services that they perform and engage in the process to notify line management upon identifying any potential conflict. The Company encourages its clients to periodically review this Client Conflict of Interest Policy so that they are always aware of what information the Company collects, how it uses it and to whom it may disclose it, in accordance with the provisions of this Policy.

4.5. Client's Consent

By entering into a Client Agreement with the Company for the provision of online gambling services, the Client is consenting to an application of this Policy on him.

In the event that the Company is unable to deal with a conflict-of-interest situation it shall revert to the Client.

5. RECORD KEEPING POLICY

The Company shall arrange for records to be kept of all services provided and transactions undertaken by the Company as well as records related to its business and internal organization. The retention of the documentation, other than the original documents that are kept in hard form, may be in other forms, such as electronic form. The Company shall implement effective procedures in order to be able to retrieve the documentation without undue delay.

The Company shall have in place the following record keeping procedures in order to ensure compliance with the legal requirements:

- a) For client's account opening documentation, a copy or the references of the evidence required is kept for at least five years after the business relationship with the respective client has ended.
- b) For business relationships and transactions, the supporting evidence and records, consisting of the original documents or certified copies for a period of at least five years following the carrying out of the transaction or the end of the business relationship.
- c) Financial and other accounting data is required to be kept for tax purposes for at least 10 years after the end of such relationship;
- d) Where appropriate, the Company must consider retaining certain records e.g. customer identification, account files, business correspondence, and internal and external reports relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations.

Moreover, the Company shall arrange for the following documentation to be kept in files:

- (a) Client documentation:
 - Client agreement
 - Due diligence documentation collected during the account opening process
- (b) Outsourced functions/services:
 - Outsourcing agreement
 - Due diligence documentation related to the service provided
 - Correspondence with the regulator(s), if any
- (c) Client complaint or grievances:

- Client complaints or grievances received
 - Report prepared by the Company stating the facts and the course of action
 - Correspondence between the client and/or the regulator, if any
- (d) Employees:
- Employees agreement
 - Due diligence documentation
 - Evidence of license to offer online gaming services, if necessary and if any

Record Keeping Obligations:

The Company shall maintain appropriate records to establish an audit trail for the purposes of criminal investigation.

All documentation shall be prepared and stored (whether by original documents, copies or on microfiche or other accessible computerized form) in such a manner that they are accessible within a reasonable time and readily available to comply with any court orders or directives regarding disclosure of information or confiscation of assets.

- (a) Where practicable, appropriate evidence of client identification, account opening or new business documentation and adequate records identifying relevant financial transactions shall be kept for a period of five years following the closing of an account or the end of the transactions or the termination of the business relationship.
- (b) Where there has been a report of a suspicious transaction or the Company is aware of a continuing investigation into money laundering or other criminal activity relating to a client or a transaction, records relating to the transaction or the client shall be retained until confirmation is received that the matter has been concluded.

6. BUSINESS CONTINUITY POLICY

6.1 Policy

The Company shall establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to its systems and procedures, the preservation of essential data and functions, and maintenance of online gaming services and activities, or where that is not possible, the timely recovery of such data and functions and the timely resumption of its online gambling services and activities.

The business continuity policy shall be reviewed and approved by the Board. The policy shall be regularly being reviewed and updated.

6.2 Continuity of IT systems

The IT Department shall establish procedures to ensure that in situations of an interruption to the Company's systems (support, telephones, etc.) and procedures, the following are met:

- (a) Preservation of essential data and functions.
- (b) The maintenance of providing its online gambling services and activities.
- (c) At least the timely recovery of such data and functions and the timely resumption of its online gambling services and activities.

The Company shall identify specific systems which shall be considered as core systems required to ensure business continuity. These systems shall ensure:

- (a) The continued and uninterrupted access to the internet.
- (b) The continued and uninterrupted operation of the Gaming Platform.

7. OUTSOURCING POLICY

Outsourcing and Company's responsibility

When the Company outsources critical or important operational functions or any online gaming services or activities, it remains at all times fully responsible for discharging all of its obligations under the legal framework. When outsourcing, the Company has in place arrangements to comply with the following conditions:

- (a) Outsourcing does not result in the delegation by Senior Management of its responsibility.
- (b) The relationship and obligation of the Company towards its clients under the legal framework is not altered.
- (c) The conditions with which the Company must comply in order to be authorized are in accordance with the legal framework and are not undermined.
- (d) None of the other conditions subject to which the Company's authorization was granted is being removed or modified.

In the case that outsourcing would conclude to the transfer of functions of the Company to such degree which renders the Company a letter box entity, this is considered to undermine the conditions for authorization of the Company, according to the legal framework.

The Company shall exercise due skill, care and diligence is exercised when entering into, managing or terminating any arrangement for the outsourcing of critical or important operational functions or of any online gaming services or activities.

The respective rights and obligations of the Company and of the service provider shall be clearly allocated and

set out in a written agreement.

In case the Company and the service provider are members of the same group, the Company shall make sure that the Company controls the service provider and has the ability to influence its actions.

8. PRIVACY POLICY

8.1 Our Commitment

The Company shall take measurable steps to protect the confidentiality, security and integrity of client information.

8.2 Collection of Information

When opening an account with the Company, the Company shall collect information directly from client (in the completed Account Opening Application Form or other way) or from other persons including, for example, credit reference agencies, fraud prevention agencies, banks, other financial institutions, third authentication service providers and the providers of public registers. This information includes, but is not limited to personal details such as name, address, date of birth, contact details, payment details, including credit card, debit card and bank account details, and other necessary financial information.

The Company might also collect information in regard to the use of our website(s), such as pages visited, frequency, duration of visit and gaming activities.

From time to time the Company may also request further information to help improve Service under the relevant Agreement, as the case may be, or comply with the applicable Laws and Regulations.

8.3 Use of the Information.

The Company shall store, process, and handle Personal Information of natural persons clients in connection with the furthering of the agreement with the clients.

The information (not in the public domain or already possessed by the Company without a duty of confidentiality) which the Company hold shall be treated by the Company as confidential and will not be used for any purpose other than in connection with the provision, administration and improvement of its Services or the furthering of the agreement with clients, establishing and managing the account or a relationship , reviewing clients' ongoing needs, enhancing customer service and products, giving clients ongoing information or opportunities that the Company believes may be relevant to them, improving relationship, anti-money laundering and due diligence checks, for research and statistical purposes and for marketing purposes (according to the relevant agreement in place), as applicable.

8.4 Contacting Clients

The Company, for the purpose of administering the terms of its agreement with clients, from time to time, make direct contact with clients by telephone, online chat, email, or post.

The Company or any of its Affiliates or group company, may make contact with clients from time to time, by telephone, online chat, email or post for marketing purposes to bring to their attention products or services that may be of interest to them or to conduct market research.

8.5 Disclosure of Information

Under the agreement with clients, the Company has the right to disclose client information (including recordings and documents of a confidential nature, card details) in certain circumstances. According to the agreement, the information may be disclosed:

- (a) Where required by law or a court order by a competent Court.
- (b) Where requested by our supervising regulatory authority having control or jurisdiction over the Company or its associates or the client or in whose territory the Company has clients or service providers, as applicable.
- (c) To relevant authorities to investigate or prevent fraud, money laundering or other illegal activity.
- (d) A Broker so as to execute the Instructions or Orders and for purposes ancillary to the provision of the Company's Services to clients.
- (e) To credit reference and fraud prevention agencies, third authentication service providers, banks and other financial institutions for credit checking, fraud prevention, anti-money laundering purposes, identification or due diligence checks of clients. To do so they may check the details client supplied against any particulars on any database (public or otherwise) to which they have access. They may also use client details in the future to assist other companies for verification purposes. A record of the search will be retained by the Company.
- (f) To the Company's professional advisors provided that in each case the relevant professional shall be informed about the confidential nature of such information and commit to the confidentiality herein obligations as well.
- (g) To other service providers who create, maintain or process databases (whether electronic or not), offer record keeping services, email transmission services, messaging services or similar services which aim to assist us collect, storage, process and use information or get in touch with clients or improve the provision of the Company's services or activities under the agreement with clients.
- (h) To data reporting service providers.
- (i) To other service providers for statistical purposes in order to improve our marketing, in such a case, the data will be provided in an aggregate form;
- (j) To market research call centers that provide telephone or email surveys with the purpose to improve our Services or activities, but only contact details. For the avoidance of doubt no payment details such as but not limited to credit card, debit card and bank details will be transmitted.
- (k) Where necessary in order for us to defend or exercise our legal rights to any court or tribunal or arbitrator or Ombudsman or governmental authority, as the case may be.
- (l) At your request or with your consent.
- (m) To affiliates or any other company in our group excluding payment details such as but not limited to credit card, debit card, and bank account details.
- (n) To employees so as to exercise their duties to further the agreement with client, or to assure the efficient functioning of the Gaming Platform.

8.6 Safeguard Measures

Client information is stored on secure servers.

The Company shall limit access of information only to those employees or partners that need to know the information in order to enable the carrying out of the agreement.

There shall be procedures in place regarding how to safeguard and use information, for example by requesting our Affiliates and employees to maintain the confidentiality of client information.

The Company shall not keep information for any longer than is required. In many cases, information must be kept for considerable periods of time. Retention periods will be determined taking into account the type of information that is collected and the purpose for which it is collected, bearing in mind the requirements applicable to the situation and the need to destroy outdated, unused information at the earliest reasonable time. In any event, the Company will keep information for the duration of applicable Laws and Regulations as a minimum.

While the Company shall use all reasonable efforts to safeguard client information, the use of the internet is not entirely secure and for this reason we cannot guarantee the security or integrity of any personal data transferred from clients, or to clients via the internet.

9. COMPLIANCE POLICY

9.1 Policy

The Company will establish, implement and maintain adequate policies and procedures designed to detect any risk that may arise and put in place adequate measures and procedures designed to minimize such risk for range of online gambling services and activities undertaken in the course of that business.

The Company shall establish and maintain a permanent and effective compliance function which shall operate independently.

In order to enable the compliance function to discharge its responsibilities properly and independently, the Company shall ensure that the following conditions are satisfied:

- (a) Ensure that the compliance function has the necessary authority, resources, expertise and access to all relevant information so as to ensure that the compliance function is exercising its responsibilities properly and independently.
- (b) Ensure that a CO/MLRO is appointed and responsible for the compliance function.
- (c) Ensure that the relevant persons involved in the compliance function must not be involved in the performance of services or activities monitored by the department.
- (d) Ensure that the method of remuneration of the relevant persons involved in the compliance function does not compromise their objectivity and must not be likely to do so.
- (e) Record any changes in the Company's operations, notify the respective regulator of the changes, and amend any legal and compliance documents so as to be up to date with the operations of the Company.
- (f) Identify any potential conflict of interest situations, and attempt to resolve it in a timely and efficient manner.
- (g) Keep records of any conflict of interests situations occur in the Company.
- (h) Assist the board of directors by evaluating and reporting to them the effectiveness of the controls for which they are responsible.
- (i) Perform periodically reviews on the procedures followed by the employees to ensure compliance with the Law and Regulations and Manual.
- (j) Review and where necessary update the Manual.
- (k) Review randomly clients' files to ensure that the account opening procedure is properly implemented and that adequate records are kept by the Company.
- (l) Review randomly the clients' accounts with special consideration to the recording process of deposits/withdrawals and clients' transactions.
- (m) Update the staff and management of the Company regarding new legislation.
- (n) Submit the annual report to Board of Directors over the activities of the Department, with special consideration to appropriate remedial measures that have been taken over the year in the event of any deficiencies.
- (o) Ensure that the performance of multiple functions by the Company's relevant persons does not and is not likely to prevent those persons from discharging any particular function soundly, honestly, and professionally.

The appointment of the CO/MLRO will be the responsibility of the Board of Directors.

9.2 Reporting Obligations:

- (a) The Company shall annually and within a period to be determined by the GCB, following the end of the financial year, submit to the GCB their annual accounts which contain at the least a balance sheet and a profit-and-loss account, accompanied by an explanatory statement with regard to the preceding financial year.

- (b) The annual accounts of the Company shall be accompanied by a statement with regard to the accuracy of the annual accounts issued by an external expert, and a management letter.
- (c) The GCB may set out generally binding provisions with regard to the contents of the annual accounts and the form and manner in which they must be submitted, which the Company shall endeavor to adhere to.
- (d) The GCB may grant full or partial dispensation from the obligations, referred to in the Paragraphs (a) through Restrictions and requirements may be set out with regard to the dispensation. The Company shall remain in compliance with the requirements and restrictions set out regarding the dispensation, referred to in the first sentence of this paragraph (d).
- (e) The Company shall have the obligation to publish their annual accounts for the preceding financial year, within a term to be determined by the GCB and in a form to be determined by the GCB.
- (f) The GCB may set out further generally binding provisions with regard to the publication of the annual account referred to in paragraph (e) and the manner of publication, which the Company shall endeavor to adhere to.
- (g) In addition, the Company shall periodically submit to the GCB any information that is reasonably needed for the fulfillment of their duties by virtue of NOOGH, in accordance with the generally binding provisions set by the GCB with regard to the contents of the referred information and the form, manner, periodicity and the terms of submission, as well as with regard to the certification of said information by an external expert.

10. AML POLICY

The provisions of the aforesaid section shall be read in conjunction with the provisions of the Compliance AML Program established by the Company.

10.1 Duty to cooperate for prevention of Money Laundering and other criminal activities

- (a) ~~The Company~~ shall comply with the guidelines and directions issued by the GCB or other competent authority for the implementation of the legislative requirements.
- (b) The Company shall determine the identity of the beneficial ownership of all their clients' accounts and shall not open or maintain such accounts, unless they are satisfied of this requirement, as stipulated in the Manual and Laws and Regulations.
- (c) The Company shall take all reasonable measures to ensure that accounts are not used for the purpose of holding assets obtained as the result of, or for facilitating the commission of any criminal activity or for any purpose contrary to the applicable legislation and regulations.
- (d) The Company shall develop and implement policies and procedures to identify and avoid money laundering transactions and to ensure compliance with the requirements of Manual and Laws and Regulations; and such policies shall include an appropriate training program for their staff.
- (e) The Company shall, on a regular basis, evaluate the effectiveness of their policies and control procedures in complying with the legislative requirements and any relevant guidelines, and such evaluation shall be an integral component of any audit.
- (f) The Company shall be vigilant in ensuring the prevention of their involvement or misuse in money laundering activities, and shall not knowingly accept assets or enter into business relationships where there is reasonable cause to believe that such assets may have been acquired illegally or that they represent the proceeds of criminal activity.

The Company shall establish procedures to obtain appropriate evidence of client identity, and shall maintain adequate records of client identity and transactions involved in such a manner as to assist, if necessary, in the investigation of criminal offences.

10.1.1 The role of the Board

- (a) The Board has the ultimately responsibility for the effectiveness of the Company's AML/CFT framework. The Board's oversight role is intended to ensure, inter alia, that there is compliance with all the relevant laws and regulations and international standards. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.
- (b) The Board and the Senior Management should be aware that:
 - i. The use of a group-wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the Company and compliant with Manual and Laws and Regulations. Failure to ensure compliance by the Company with the legal requirements may result in significant penalties for directors and the financial institution.
 - ii. Subsidiaries and branches of the Company, if applicable, including those domiciled outside of Curaçao are expected to, at a minimum, comply with the AML/CFT requirements of the Manual and Laws and Regulations; and
 - iii. Where some of the Company's operational functions are outsourced out of Curaçao, the counter parties are expected to, at a minimum, comply with the AML/CFT requirements of the Manual and Laws and Regulations.
- (c) The Board should therefore demonstrate its commitment to an effective AML/CFT program by:

- i. Understanding the statutory duties placed upon it, their staff and the entity it represents;
- ii. Approving AML/CFT policies and procedures that are appropriate for the risks faced by the Company. Evidence of consideration and approval of these policies should be reflected in the board minutes and noted in the policy;
- iii. Appointing an individual within the organization to ensure that the Company's AML/CFT procedures are being managed effectively; and
- iv. Seeking assurance that the Company is in compliance with its statutory responsibilities as it relates to AML/CFT. This includes reviewing the reports from compliance on the operations and effectiveness of compliance systems.

10.1.2 The role of the Senior Management

Senior management is responsible for the development of sound risk management programs and for keeping the Board adequately informed about these programs and their effectiveness. These programs, which should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments, should be formally documented and, at a minimum, irrespective of whether the Company receives funds from third parties or not, should provide for:

The development of internal policies, procedures and controls for, *inter alia*:

- (a) The opening of customer accounts and verification of customer identity.
- (b) Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers).
- (c) Determining business relationships that the Company will not accept by requiring graduated customer acceptance policies and procedures with more extensive due diligence for higher risk customers.
- (d) Determining an exit strategy to terminate undesired relationships with existing customers.
- (e) The timely detection of unusual activities and reporting of suspicious transactions to the FIU.
- (f) Internal reporting.
- (g) Records retention.

The recruitment of a level of staff, appropriate to the nature and size of the business, to carry out identification, research of unusual transactions and reporting of suspicious activities:

- (a) Designation of a CO/MLRO at an appropriate level of authority, seniority and independence to coordinate and monitor the compliance program.
- (b) An ongoing training program designed to ensure employees adhere to the legal and internal procedures and become familiar with the dangers they and the business entity face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks.
- (c) Establishment of management information/reporting systems to scrutinize customer account activity and facilitate aggregate and group- wide monitoring of significant balances regardless of whether the accounts are held on balance sheet, as assets under management or on a fiduciary basis.
- (d) An effective independent risk-based oversight function to test and evaluate the compliance program.
- (e) Screening procedures for hiring, and ongoing systems to promote high ethical and professional standards to prevent the Company from being used for criminal activity. This should include but is not limited to enquiries about the personal history of the potential employee and verifying appropriate references on the individual.

Policies should be periodically reviewed for consistency with the business model, and product and service offering. Special attention should be paid to new and developing technologies.

10.2 Customer Acceptance Policy

The Company shall maintain clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher-than-average risk. Before accepting a potential client, KYC and due diligence procedures are followed, by examining the following factors:

- customers' background
- country of origin
- Public or high-profile position (i.e. PEPs)
- linked accounts
- Business activities
- Any other risk indicators.

Enhanced due diligence is essential for an individual with high net worth but whose source of funds is unclear. New clients' money is transferred through a reputable bank. Banks have their own anti-money laundering procedures. A decision to enter into business relationships with higher risk customers, such as politically exposed persons, is taken exclusively at senior management level.

Company's operations procedures in terms of accepting new clients and compliance requirements, accepting funds and withdrawal procedures:

- Compliance department oversees the provided documents in order to identify and verify the client
- depositing method must be examined so that there will be no suspicious activity and in order to comply with the Anti Money Laundering protocols.

10.3 Recognition and Reporting of Suspicious Transactions.

- (a) The Company shall promptly report suspicious transactions relating to any account to the FIU.
- (b) The Company shall pay special attention to all complex, unusual or large business transactions, or unusual patterns of transactions whether completed or not, and to insignificant but periodic transactions, which have no apparent economic or lawful purpose.
- (c) Upon reasonable suspicion that the transactions described in paragraph (b) above could constitute or be related to money laundering, or other criminal activities, the Company shall promptly report the suspicious transactions to the FIU on the GoAML platform.
- (d) The Company shall not notify any person, other than a court, competent authority or other person authorised by law, that information has been requested by or furnished to a court or the FIU.
- (e) Where a report referred to in paragraph (iii) above is made in good faith, the Company and its employees, staff, directors, owners or other representatives as authorised by law, shall be exempted from criminal, civil or administrative liability, as the case may be, for complying with this regulation or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, regardless of the result of the communication.
- (f) Where there is suspicion that the source of funds may be criminal or that a client may be involved in criminal activity, the Company shall follow established procedures for assessing the evidence and determining what course of action should be pursued.
- (g) The Company, depending on the nature of the suspicion, decide whether or not they can continue

the business relationship or whether they should subject it to particular scrutiny or undertake further investigation, and consideration shall be given to whether or not it is appropriate to make a report to the FIU.

- (h) The Company shall make a report in any case in which he knows that funds are connected with criminal activity.
- (i) The Company shall be aware that suspicions shall depend upon the nature of the relationship and the transaction and the particular circumstances of each case, and there is no one test that may be applied to determine what constitutes a suspicious transaction but an understanding of the client's business and adequate record keeping shall facilitate the assessment.
- (j) For the purpose of clarification, unsatisfactory explanation or lack of commercial rationale, unusual patterns of transactions and inconsistency with the client's business may be indicia that a transaction or a series of transactions should be subjected to particular scrutiny.
- (k) The Company shall have internal procedures to ensure that suspicions about the source of funds or transactions are reported to the FIU and they shall be aware of the importance of cooperation with the FIU and the GCB.
- (l) The Company shall keep records of reports made by their staff and of reports made to the FIU.
- (m) Where a report has been made to the FIU, the Company and their staff shall be aware of the dangers of impeding an investigation into money laundering or other criminal activity by tipping off the client or others.
- (n) The Company shall cooperate fully with law enforcement authorities and the Commission to ensure that money laundering or other criminal activities are fully investigated and prosecuted.
- (o) Where the Company has reason to believe that a client is requesting services in order to facilitate criminal activities, he shall withhold the performance of such services.

10.4 Customer Due Diligence

10.4.1 In accordance with the Manual and Laws and Regulations, the Company shall establish the identity and verify the identity of any customer of the Company by requiring the customer to produce an identification record or such other reliable, independent source document.

- a) The requirements of subsection (a) shall apply when:
 - i. the Company establishes a business relationship.
 - ii. in the absence of such a relationship, the Company conducts:
 - any transaction in an amount equal to or above the sum as prescribed by the Laws and Regulations, whether conducted as a single transaction or several transactions that appear to be linked and where the amount of the transaction is unknown at the time of the transaction, the identification and verification shall be undertaken as soon as the amount becomes known or the said threshold is reached.
 - any wire transfers.
 - iii. there is a suspicion of money laundering or terrorist financing; or
 - iv. the Company has doubts about the veracity or adequacy of previously obtained customer identification data.
- b) Without limiting the generality of subsection (a), the Company shall:
 - i. When establishing a business relationship, obtain information on the purpose and nature of the business relationship and the source of funds;
 - ii. if the transaction is conducted by a natural person, adequately identify and verify his identity including information relating to:
 - the person's name and address ;
 - the national identity card, social security document, passport or other applicable official identifying document;

- the source of funds;
- iii. if the transaction is conducted by a legal person or legal arrangement, obtain information on that legal person or legal arrangement, adequately identify the company, the beneficial owner and ultimate natural persons providing the funds of such legal person or legal arrangement and take reasonable measures to identify and verify the legal status, ownership and control structure, including information relating to:
- proof of incorporation or similar evidence of establishment or existence; and;
 - the customer's name, name of trustee and ultimate settler (for trusts) and of persons providing funds and council members (for foundations), legal form, head office address and identities of directors (for legal persons) and source of funds;
- iv. have appropriate risk management systems to determine if a potential customer, customer or beneficial owner is, is likely to be, is found to be or becomes a Politically Exposed Person* ("PEP"), and if so, shall:
- adequately identify and verify his identity as set out in this section;
 - obtain the approval of senior management before establishing or continuing a business relationship with the politically exposed person;
 - take reasonable measures to establish the source of funds and source of property; and
 - conduct regular enhanced ongoing monitoring of the business relationship.
- v. perform due diligence measures on a risk sensitive basis which are consistent with the Manual; and
- vi. upon the establishment of a business relationship, and when completing the verification of the identity of the customer and beneficial owner, ensure that money laundering risks are effectively managed.

*The definition of "Politically Exposed Person" (as per Laws and Regulations) includes a Foreign PEP, a Domestic PEP or an International Organization PEP as defined below:

"Domestic PEP" means a natural person who is or has been entrusted domestically with prominent public functions in Curaçao and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

"Foreign PEPs" means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

"International Organization PEP" means a person who is or has been entrusted with a prominent function by an international organization and includes members of senior management or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

It shall also include the following:

- Current/former Rulers, Kings, Queens, and their relatives, friends, and other close associates.
- Connected Persons, i.e. those connected to or associated with a public official who may receive tainted funds on behalf or as a result of their connection with that PEP. Such persons may also include: immediate family (spouses, children, parents, brothers/sisters); aides and other close advisers; business associates; an individual who owns, operates or exercises significant control in relation to any business activities including casinos, money transfer, bureaux de change or companies involved in the production or distribution of arms and military products etc.

The above list must not be viewed as being exhaustive and judgment must be exercised in determining whether other categories of individuals who exercise significant influence in political/public sectors should be treated as PEPs.

- c) The Company shall, in relation to its higher risk category of customers or business relationship, conduct annual reviews of its record to ensure that the documents, data or information obtained pursuant to subsection (iii) is kept up- to-date and relevant.
- d) If it appears to the Company that an applicant requesting it to enter into any business relationship or transaction, whether or not in the course of a continuing business relationship, is acting on behalf of another person, the Company shall establish the true identity of any person on whose behalf or for whose ultimate benefit the applicant may be acting in the proposed transaction, whether as a trustee, nominee, agent or otherwise.
- e) Nothing in this section shall require the production of any evidence of identity where the customer is itself a financial institution to which the AML/CFT laws applies and which has been licensed or registered, and is supervised for anti-money laundering and countering the financing of terrorism measures by a regulatory authority and the Company has satisfied itself as to the adequacy of the measures to prevent money laundering and the financing of terrorism; or there is a transaction or a series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.
- f) Where the Company relies on an intermediary or third party to undertake its obligations under subsections (i), (ii) or (iii) or to introduce business to it:
 - i. must be satisfied that the third party is able to provide copies of identification data and other documents relating to the obligation of due diligence under subsections (i), (ii) and (iii) without delay;
 - ii. shall satisfy itself that the third party or intermediary is regulated and supervised, and has AML/CFT measures in place to comply with the requirements set out in the Manual and Laws and Regulations in accordance with the Financial Action Task Force recommendations on regulation, supervision and monitoring.
 - iii. shall immediately obtain from the third party, copies of identification data and other documents relating to the obligation of the customer due diligence process;
 - iv. shall ensure countries where third parties are based adequately apply the Financial Action Task Force recommendations;
 - v. shall maintain ultimate responsibility for customer identification and verification of customer.
 - vi. Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, which for the purposes of this Manual are the physical identity (e.g. name and date of birth) and the activity undertaken.
- g) The Company must avoid the acceptance of anonymous accounts or accounts in fictitious names.

- h) As part of the due diligence process, the Company should:
 - a. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset of a business relationship. This process should include, where appropriate:
 - i. Taking reasonable measures to understand the ownership and control structure of the customer;
 - ii. Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and
 - iii. Discontinuing the transaction, if customer documentation information is not forthcoming at the outset of the relationship.
 - b. Employ enhanced due diligence procedures for high risk customers or transactions or business relationships such as private banking operations, non-resident customers, trust arrangements, companies having nominee shareholders or customers who the financial institution has reasons to believe are being refused banking facilities by another financial institution
- i) The following original documents are acceptable methods for confirmation of the identity of local customers:
 - i. Valid government-issued photo-bearing identification (e.g. passport, Social Security Card, Voter's ID, Driver's license along with a social security card or passport);
 - ii. Valid Armed forces ID card;

The above should contain a validity date.

- j) The following original documents are acceptable methods for confirmation of the current permanent address of local customers:
 - a. Government-issued identification;
 - b. Utility bill;
 - c. Tax bill;
 - d. Bank or credit card statement;
 - e. Letter from a Judge or Magistrate of a Court;

The above should be less than 3 months old.

10.4.2 KYC Documentation For Natural Persons

- a) The Company must obtain and document the following basic information when seeking to verify identity:
 - i. True name/names used and correct permanent residential address including postcode (if applicable);
 - ii. Valid photo-bearing identification, with unique identifier, (e.g. passport, social security card or driver's license along with a passport or social security card);
 - iii. Date and place of birth and nationality (indication should be made if dual citizenship is maintained);
 - iv. Contact details e.g. telephone number, fax number and e-mail address;
 - v. Signature;
 - vi. Purpose of the account and the nature of the business relationship.
- b) The following information may also be required when the Company seeks to verify identity:
 - i. Occupation and name of employer (if self-employed, the nature of the self-employment);

- ii. Estimated level of account activity including:
 - 1. Size in the case of online gaming wagering and custody accounts;
 - 2. Balance ranges, in the case of current and deposit accounts;
 - 3. An indication of the expected transaction volume of the account;
 - iii. Source of funds; and
 - iv. Any other information deemed appropriate and relevant.
- c) Identification documents, either original or certified copies, should be pre-signed and bear discernible photograph of the applicant, for example:
- i. Current valid passport;
 - ii. Armed forces ID card;
 - iii. Driver's license bearing the photograph and signature of the applicant (to be used along with a passport or social security card);
 - iv. Voter's card;
 - v. Social security card; or
 - vi. Such other documentary evidence as is reasonably capable of establishing the identity of the individual customer.
- d) One or more of the following steps used in order to confirm customer's addresses:
- i. Checking the Register of Electors (where available);
 - ii. Provision of a recent utility bill, tax assessment or bank/credit card statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
 - iii. Checking the telephone directory; and
 - iv. Record of home visit (where possible).
- e) Where prospective customers provide documents with which the Company is unfamiliar, either because of origin, format or language, the financial institution must take reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining a notarized translation.
- f) In circumstances where the Company's customer is considered a high-risk client, the Company should also take reasonable measures to establish the customer's source of wealth and document findings.
- g) Where a customer is unable to produce original documentation needed for identification or verification, copies should be accepted if certified by persons listed in section 11.5 of this Manual.

10.5 Customers' Profile Policy

A customer profile policy is determined and implemented under particular criteria related with clients risk profile. In particular the factors that specify the risk category at which a client is attributed are mainly dealing with client:

- a) The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);
- b) The nature and frequency of the activity;
- c) The complexity, volume and pattern of transactions;
- d) Type, status and value of account;
- e) Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);
- f) Type of product/service;
- g) Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash withdrawals);

- h) Geographical origin of the customer;
- i) Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);
- j) Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
- k) Unwillingness of the customer to cooperate with the financial institution's customer due diligence process for no apparent reason;
- l) Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

10.6 Risk Based Approach

- a) The Company's risk-based approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective program. This should be evidenced by categorization of the customer base, products and services by risk rating and identification of assigned actions by risk types.
- b) Prior to establishing a business relationship, the Company should assess the potential risk inherent in each new client relationship. This assessment should take into account the products or facilities to be used by the customer and whether and to what extent a customer may expose the Company to risk. The financial institution should then decide whether or not to establish or continue with a relationship.
- c) The Company categorizes customers in terms of risk in 3 groups, namely:
 - i. Low Risk
 - ii. Medium Risk
 - iii. High Risk
- d) The Company's risk-based approach take into account customer acceptance and on-going monitoring policies and procedures that assist the Company in identifying the types of customers that are likely to pose higher than average money laundering and terrorist financing risk.
- e) The Company is required to risk rate all client relationships including those in existence prior to the implementation of these Guidelines. All risk ratings should be documented and should be in place for all customers.
- f) The Company adopted reasonable criteria for assessing the risks (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place).
- g) The Company conducts periodic reviews (however, not more than two years apart) to determine whether any adjustment should be made to its risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

10.7 Simplified Customer Due Diligence

Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems.

10.8 Enhanced Customer Due Diligence

- a) A more extensive customer due diligence process should be adopted for higher risk customers. In particular, the Company applies enhanced due diligence to customers where the risk of being used for money laundering or terrorist financing is high. It follows, then, that simplified customer due diligence measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.
- b) The Company may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A financial institution may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries.
- c) Applying a risk-based approach, enhanced due diligence for high-risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:
 - i. An evaluation of the principals;
 - ii. A review of current financial statements;
 - iii. Verification of the source of funds;
 - iv. Verification of source of wealth;
 - v. The conduct of reference checks;
 - vi. Checks of electronic databases; and
 - vii. Periodic reporting to the Board about high-risk accounts.
- d) The Company should give particular attention to the following business relations and transactions:
 - i. Where a customer has not been physically present for identification purposes;
 - ii. Correspondent relationships;
 - iii. Business relationships or occasional transactions with a PEP;
 - iv. Business relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML measures;
 - v. Corporate customers able to issue bearer shares or bearer instruments.
- e) In particular, the Company defines the following types of customers as high-risk clients and therefore enhanced due diligence are applied:
 - i. Non-Profit Organizations
 - ii. Non-Face to Face Customers
 - iii. Introduced Business
 - iv. Professional Service Providers
 - v. Politically Exposed Persons
 - vi. High-Risk Countries
 - vii. Bearer Shares
 - viii. Correspondent Banking

10.9 Other obligations of the Company

- a) The Company shall establish and maintain the following:

- i. records of all transactions in accordance with the requirements of subsection (iii) below
 - ii. where evidence of a person's identity is obtained, a record that indicates the nature of the evidence obtained, and which comprises either a copy of the evidence or such information as would enable a copy of it to be obtained;
 - iii. account files and business correspondence in relation to accounts;
 - iv. written reports established in accordance with section 11.6 of this policy.
- b) Customer accounts of the Company shall be kept in the true name of the account holder.
- c) Records required under subsection (i) shall contain particulars sufficient to identify:
 - i. the name, address and occupation or, where appropriate, business or principal activity of each person conducting the transaction; or
 - ii. if known, on whose behalf the transaction is being conducted, as well as the method used by the Company to verify the identity of each such person;
 - iii. the nature and date of the transaction;
 - iv. the type and amount of currency involved;
 - v. the type and identifying number of any account with the Company involved in the transaction;
- d) Records required under subsection (i) shall be kept by the Company for a period of at least 7 years from the date the relevant business or transaction was completed, or termination of business relationship or any longer period if requested by the FIU in specific cases and upon proper authority and the requirement to keep the record shall apply whether the account or business relationship is ongoing or has been terminated. In addition,
 - a) The FIU may, in writing, require from the Company to keep a record for a specified period of time;
 - b) The Company shall keep such records of a transaction that are sufficient to permit reconstruction of individual transactions;
 - c) Any record kept under this section, shall be maintained in a manner for use as evidence for prosecution of an offence.
- e) The Company shall ensure that customer information and transaction records are available on a timely basis to authorities upon proper authority.
- f) The receiving intermediary or third party financial institution shall keep all records received from an ordering financial institution where technical limitations would prevent the full originator information that should accompany a cross border wire transfer from being transmitted with a related domestic wire transfer for five years.
- g) The Company shall:
 - i. comply with any instruction issued to it by the GCB or any other competent body.
 - ii. permit any authorized officer of the GCB or any other competent body to enter into any premises of the Company during normal working hours and inspect the records kept pursuant to the provisions of subsection (i) of this section and make any notes or take any copies of the whole or any part of any such record and shall answer any questions of the GCB or any other competent body in relation to such records;
 - iii. comply with the guidelines and training requirements issued and provided by the GCB or any other competent body.
- h) The Company is prohibited from conducting any banking business such as receiving money from the public through the acceptance of deposits on current account, deposit account or other similar accounts which may be withdrawn on demand by cheque, draft, order or notice by customers and using that money to make advances, loans, extensions of credit, guarantees and investments.

10.10 Reporting Of Suspicious Transactions By The Company

- i. The Company shall pay special attention to:
 - a) all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not, and to insignificant but periodic transactions, that have no apparent economic or lawful purpose;
 - b) business relations and transactions with persons including legal persons and arrangements, from or in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or terrorist financing;
 - c) electronic funds transfer that do not contain complete originator information and shall adopt effective risk-based procedures to identify and handle any such transfer.
- ii. The Company shall conduct ongoing due diligence on its business relationships and scrutinize transactions undertaken throughout the course of the relationship to ensure that its obligations under the relevant section of the Manual and the Laws and Regulations are met and that the transactions being conducted are consistent with information that the Company has of its customer and the profile of the customer's business and where necessary the source of funds.
- iii. Whenever the Company suspects or has reasonable grounds to suspect that any transaction, proposed transaction or attempted transaction is related to the commission of a money laundering offence or terrorist financing offence or is related or linked to, or is to be used in connection with a terrorist act or for the financing of terrorism, or that the funds or property are the proceeds of crime, it shall as soon as possible but not later than 14 days after forming that suspicion and wherever possible before the transaction is carried out:
 - a) take reasonable measures to ascertain the purpose of the transaction, the origin and ultimate destination of the funds involved and the identity and address, of any ultimate beneficiary;
 - b) Make an internal STR to the MLRO/DMLRO
 - c) On receipt of the internal STR, the MLRO will acknowledge receipt. The STR will be reviewed in the light of the information provided plus any other relevant information that is obtained.
 - d) The MLRO shall decide whether to file the report with the FIU in the GoAML platform. A copy of all records lodged with the FIU will be kept by the MLRO separate from the client's file. Copies of documentation surrounding the suspicious transaction may be submitted to the FIU.
- iv. If the Company has reported a suspicious transaction in accordance with this section shall, if requested to do so by the FIU, give such further information as requested by the FIU.
- v. The Company to establish and maintain a register of all ML/TF internal disclosures made to the MLRO or Deputy MLRO. The register must include details of:
 - the date the report was made.
 - the person who made the report.
 - whether the report was made to the MLRO or Deputy MLRO.
 - information to allow the papers and relevant documentation to be located.

The Laws and Regulations requires the relevant person to establish and maintain a register of all ML/TF external disclosures made to the FIU. The register must include details of:

- the date of the disclosure.
- the person making the disclosure.
- information to allow the papers relevant to the disclosures to be located.

10.11 Company To Appoint A Compliance Officer And Establish Procedures, Etc.

As part of its compliance arrangements, the Company is responsible for appointing a CO who is responsible for the implementation and ongoing compliance with internal programs, controls and procedures in accordance with the requirements of the Laws and Regulations.

The CO must:

- be a natural person.
- be of at least senior management level 18.
- be an approved officer under the Laws and Regulations.
- have the appropriate qualification knowledge, skill and experience to fulfill a compliance role within the Company.

The Company must ensure that the CO:

- has timely and unrestricted access to the records of the Company.
- has sufficient resources to perform his or her duties.
- has the full co-operation of the staff.
- is fully aware of his or her obligations and those of the Company.
- reports directly to, and has regular contact with, the Board so as to enable the Board to satisfy itself that all statutory obligations and provisions in the Laws and Regulations, the Code, and the GCB rules are being met and that the Company is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

Senior management is defined under the Laws and Regulations as an officer or employee with sufficient knowledge of the Company's ML and TF risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the Board of directors.

The functions/responsibilities of the CO (and his team) are as follows:

- ensuring continued compliance with the requirements of the Laws and Regulations subject to the ongoing oversight of the Board of the Company and Management.
- undertaking day-to-day oversight of the program for combatting ML and TF.
- contributing to designing, implementing and maintaining internal compliance manuals, policies, standards, checklists, procedures and systems for combatting ML and TF.
- supporting Management in discharging their responsibilities to comply with applicable regulations, laws, codes etc (e.g. by reviewing activities of the company, recommending systems enhancements, initiating changes to procedures and systems to reflect regulatory requirements, etc).
- Independent Compliance Reviews of client files.
- providing AML/CFT training programs.
- providing an independent reporting mechanism to the Board.
- fostering good relations with regulators.
- Compliance that equally cumulates the internal audit function, will conduct regular checks to:
 - examine all aspects of the operations including the BCP to ensure adherence to established policies, procedures, controls and other relevant laws, codes, guidelines issued by regulatory bodies.
 - conduct ad-hoc inspections as may be planned by Compliance or delegated by Management.
 - produce a report with appropriate recommendations to management for rectification of any deficiencies identified.
- s/he acts as the principal point of contact for the regulators with respect to compliance issues.
- Other risk assessments not covered above

10.11.1 Appointment of MLRO

The Company shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in ML or TF.

The MLRO shall:

- be sufficiently senior in the organization of the reporting person or have sufficient experience and authority.
- have a right of direct access to the Board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

The MLRO shall ultimately receive all internal disclosures and consider any report to determine whether an external disclosure is required.

The MLRO appointed by the Company must:

- be a natural person.
- be an approved officer under the applicable legislation.
- have the appropriate knowledge, skill and experience in accordance with the standards of the GCB.

The Company must ensure that the MLRO:

- is the main point of contact with the FIU in the handling of disclosures.
- has unrestricted access to the CDD information of the Company's customers, including the beneficial owners thereof and other relevant information on client files.
- has sufficient resources to perform his or her duties.
- is available on a day-to-day basis.
- reports directly to, and has regular contact with, the Board or equivalent of the Company.
- is fully aware of both his or her personal obligations and those of the Company Laws and Regulations, the Code, and the GCB Regulations.

The same individual can be appointed to the positions of MLRO and CO, provided the Company considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively

This arrangement shall be reviewed on a yearly basis and if required these roles shall be segregated among 2 persons.

The Company should also appoint a DMLRO in order to exercise the functions in the MLRO's absence. The DMLRO should be of similar status and experience to the MLRO. Where this Manual refers to the MLRO it implies the DMLRO in the MLRO's absence.

Both the MLRO and DMLRO shall separately register on GoAML platform of FIU so that they can independently file any required STR with the FIU.

10.11.2 Duties of MLRO

The duties of the MLRO shall be as follows

- Sets policies and standards to cover Compliance issues.
- Supports Management in discharging their responsibilities to comply with applicable regulations, laws, codes etc (e.g. by reviewing activities of the company, recommending systems enhancements, initiating changes to procedures and systems to reflect regulatory requirements, etc).
- Fosters good relations with regulators.
- Acts as the principal point of contact for the regulators including the FIU.
- Implements and monitors the day-to-day operation of the Company's compliance with the Laws and Regulations and reporting to the Board on any material breaches of the internal AML/CFT policy and procedures and other relevant laws, codes and standards of good practice.
- Acts as a central point for the receipt and validation of Internal STRs prior to reporting to the FIU within the prescribed delay.
- Reports immediately to relevant Management any material and significant breaches or potential breaches of

AML/CFT Laws and Regulations of which the MLRO is aware.

- Provides training to all staff with a view to ensuring compliance with the requirements of the GCB rules, and other AML/CFT laws are met.
- Makes annual reports or such other periodic reports as deemed necessary on the adequacy/shortcomings of internal controls and other AML/CFT procedures implemented
- Makes recommendations to the Board on necessary actions to be taken to remedy deficiencies identified by the MLRO.
- Any other duties as may be required under the Internal Control Manual or other policies including the Laws and Regulations in Curaçao.

10.11.3 Internal Audit

The CO and MLRO shall also have the role of internal audit. However, an independent audit function to test the ML and TF policies, procedures and controls of the Company shall be maintained, once the Company has reached a certain size.

PART III
DEPARTMENTAL MANUALS

1. FINANCE AND ACCOUNTING DEPARTMENT

As per Laws and Regulations, the Company should keep proper accounting records.

The Head of Finance & Accounting Department will be a qualified and experienced person and shall report to the Senior Management who shall be responsible for the supervision of the Department.

The procedures which shall be followed by the employees of this department, aim to ensure that due keeping of the books and records is properly performed and in compliance with the Laws and Regulations. In this respect, the Head of the Department will also be monitored by the CO/MLRO of the Company in order to ensure that the procedures followed by the Company are duly in line with the Manual and the Laws and Regulations. However, the major responsibilities of the Finance & Accounting Department are outlined below:

1.1 Accounts payable monitoring

Finance and Accounting Department shall be responsible for the following in relation to accounts receivable and accounts payable:

- Proceed with the payment / settlement of invoices issued by services providers, associates, provided that have been approved by Senior Management and / or have been issued in accordance with a corresponding agreement / engagement letter.
- Proceed with the investigation of invoices of large/unusual amounts which have been issued by any service provider or associates.
- Proceed with the settlement of routine payments, such as electricity, telephone etc.

1.2 Accounting Records Maintenance

The Company is obliged to keep its records including accounting records at its registered office, or at such other place as may be determined by its directors or other competent persons.

Where the company changes the place at which its records are kept, it shall, within 14 days of the change, notify the Registrar of Companies in writing of the place at which the records are kept.

1.3 Accurate records

The Company shall keep accurate and reliable and shall correctly explain and document all financial transactions so as to enable each financial transaction of the entity to be properly constructed and understood, to enable the financial position of the entity to be determined with reasonable accuracy at any time and also to enable the preparation of financial statements for such entity.

1.4 Retention of records

All accounting records shall be maintained and retained for a period of not less than seven years following the closure of an account, or the end of a transaction, or the termination of a business relationship, whether such relationship is a one-off, regular, or habitual relationship.

Copies of all suspicious transaction reports made or other reports made to FIU in accordance with the Laws and Regulations, including any accompanying documentation, shall be maintained for a period of at least 7 years from the date the report was made.

2. BACK OFFICE / ACCOUNT OPENING DEPARTMENT

The Head of the Department will be a qualified and experienced person and will be responsible for the creation, managing, and monitoring of the clients' accounts. Moreover, the Head of the Department shall report to the Senior Management of the Company who shall be responsible for the supervision of the Department.

In particular, the Back Office/ Account opening department will be responsible for the following functions:

- Open a new client account
- Maintenance of a client account
- Funds Transfer
- Deposit of incoming funds
- Withdrawal of outgoing funds
- Marketing communication

Further to the above, the Head of Department will also be monitored by the CO/MLRO of the Company in order to ensure that the procedures followed by the Company are duly in line with this Manual and the Laws and Regulations.

The procedures which are followed by the head of the department in relation to the performance of the duties are the following:

2.1. Open A New Client Account

The Department shall be responsible to ensure that all information required for the opening of an account for client are collected and are properly reviewed. The procedure followed in collecting the information is described below. The requirements of the documents to be collected are in accordance with Anti-Money Laundering Policy of the Company. In this respect the head of the department should be regularly updated for the requirements of the relevant legislation and when needed implements necessary changes to the procedures and forwards these to the Senior Management for approval.

2.2. Procedures For Client Identification

- a. The Company shall ensure that all their staff are familiar with and apply relevant procedures to verify and adequately document the true identity of clients, and for this purpose, identity will usually include a current address or place of business.
- b. The Company shall not conduct business with persons using obviously fictitious names or addresses and shall not keep anonymous accounts.
- c. Verification of identity will not normally be required in the case of an isolated transaction unless the circumstances surrounding such transaction appear on an objective standard to be unusual or questionable, in which case it will be necessary to make further enquiries.
- d. The Company may be required to take steps to verify a client's identity if money laundering is known or suspected according to the results obtained pursuant to paragraph (iii) above.
- e. Where money laundering is known or suspected under paragraphs (iii) and (iv) above, the MLRO shall not refrain from making a report to the FIU under the legal framework merely because of the size of the transaction.

2.3. Payment on an account of a financial institution

- a. Where a transaction involves payment by a client and the client does so by remitting funds from an account in a financial institution, it may be unnecessary to take any further steps to verify client identity

if the Company has evidence identifying the branch or office of such financial institution and verifying that the account is in the name of the client.

- b. Where business is placed over the telephone and payment is made in the manner specified in paragraph (i) above, the Company shall retain a record indicating how the transaction arose, in addition to a record of the relevant branch or office and the account name.

2.4. Individual Clients

- a. A prospective client shall provide his true name and permanent address and whenever possible, his date of birth shall be sought and recorded; and it will usually be appropriate to verify this information by reference to a national identity card, passport or other similar identification document, a copy of which should be retained.
- b. The Company shall take particular care to obtain adequate documentary evidence of identity in any case where prospective clients deal with them by mail or otherwise.

2.5. Accounts Maintenance

Back Office / Account Opening Department shall be responsible for carrying out the following accounts maintenance activities:

a) Archiving

All archived records must be kept for a minimum of 7 years. Documentation kept electronically will remain in the system until the client has ceased to have a relationship with the Company. When this occurs the documentation will then be stored in the archiving system as history information.

b) Deletion Of An Account

The removal of an account from the system shall be the sole responsibility of Back Office / Account Opening Department which will obtain an approval by Senior Management.

c) Closing Of A Client's Account

Back Office / Account Opening Department shall be responsible for closing a client's account under the following circumstances:

- Closing of an account upon client's request
If a client requests to close his/her account, Back Office / Account Opening Department must verify that the client provides them with clear instructions about their request in written form. In turn, funds in client's accounts shall all be withdrawn and settled within 5 working days. Note that Back Office Department must keep all records and transactions made by the client for at least 7 years after the termination of his/her account.
- Closing of an account when client has passed away
If a client has passed away, the inheritor or the person who acts on behalf of the client (e.g. lawyer) is responsible for providing instructions to the Back Office Department for closing the client's account. The Back Office Department shall also request a Death's Certificate, as well as the bank details of the inheritor(s) for transferring the underlying funds to the inheritor.

2.6. Marketing Communication

When the Company shall produce or disseminate recommendations shall ensure that is clearly identified as such. The Company shall further ensure that any such recommendation contains a clear and prominent statement that (or, in the case of oral recommendation, to the effect that) it has not been prepared in accordance with legal requirements designed to promote client understanding of the risks gambling and losing his funds.

Advertisements of the Company, either local or foreign, shall not be misleading and shall in no way compromise the reputation of Curaçao as an international online gambling center services center.

2.7. Safekeeping Department

2.7.1. Purpose

The purpose is to set out the procedures which are followed by the Company when holding clients' financial instruments and clients' funds, and to ensure its compliance with legislative requirements.

2.7.2. Withdrawal and Refund Policy

The Company shall establish policies and procedures to help ensure that all Withdrawal and Refund requests are processed efficiently and within the regulatory guidelines.

Withdrawal requests can only be submitted online via the official "Client Area" on our website. The following should be provided and/or confirmed before submitting a request:

1. the Full name (including First and last name) on the beneficiary account which must match the name on the gaming account.
2. that the withdrawal amount is less than or equal to the account balance.
3. the full details about the method used to deposit the funds, including the credit card or bank account number.
4. the full details about the method for withdrawal. Please note that the policy is to refund any funds back to the source of the original deposit.

Please note that there is a minimum withdrawal amount of 100 USD.

Processing Time Frames

In order for the Company to perform its obligations and have time to process the payment with the credit card company or bank, the below shall apply:

All withdrawals requests will be processed within 7 (seven) business days.

Please note that the Company reserves the right to review the gaming account, account history and supporting documentation before processing the withdrawal request. The Company shall also have the right to request additional information prior to completing the withdrawal request. If necessary, the Company will contact the client for further information and cancel the withdrawal request until the outstanding matters are resolved. Client will then need to re-submit the withdrawal request.

Withdrawal of Profits

Due to anti-money laundering requirements (AML) that the Company must comply with, it needs to verify that proceeds from gaming are transferred to an account where the beneficial owner is the same as on the gaming account. Therefore, it is recommended that client provides us with a copy of the bank or credit card statement where funds will be sent before you submit the withdrawal request.

Withdrawals will only be affected towards the client account and not to any other third party or anonymous account.

Receipt Of Funds

Banks and credit companies may have different internal procedures to credit funds that they receive. The Company shall not have control over when funds will be available. This would need to be communicated to clients.

For transaction confirmation, a specific email address shall be provided to clients.

Initial Deposits Processed by Debit/Credit Card

If client deposited funds using a credit card, all amounts up to the amount deposited through that same card shall be refunded. If a profit was made on the online gaming, this can also be returned through wire transfer.

In some cases, the credit card company sets time limits for issuing refunds. If this time frame expires, we will also return your funds via wire transfer. If this applies to you, please refer to the section above regarding processing.

The withdrawal process is based on strict guidelines to make sure the funds are securely sent back to their original source and beneficiary.

Withdrawal Fee

Some banks use intermediary banks that charges fees and it shall be the responsibility of client to bear those charges.

The Company may charge withdrawal fee if there is insignificant (only one single position placed on the gaming account) or no gaming activity in the client's gaming account prior to the submission of the withdrawal request.

3. INFORMATION TECHNOLOGY DEPARTMENT

The department will be outsourced to a third-party provider, whose main duty will be to ensure the Security and Integrity of:

- the network used by the Company.
- the gaming platform which is used by the Company's personnel and clients.
- the servers and personal computers of Company's personnel.

The responsibilities of the Department should be to ensure that procedures are in place regarding the following issues:

- Information Technology Security.
- Information Technology Backup.
- Building Security.

The Head of the Department shall be reporting to the Senior Management of the Company who shall be responsible for the supervision of the Department. In addition, the Department will also be monitored by the CO/MLRO of the Company in order to ensure that the procedures followed by the Company the Laws, Regulations and the Manual.

3.1. Procedures:

a) Information Technology Security

For the Company, due to the nature of its operations and activities, Information Technology Security is an important issue, and the Department shall have in place procedures to ensure the efficient and effective

application of the Information Technology Security.

The following actions shall be taken by the Department:

- Access to servers and networks firewalls is restricted only to authorized Information Technology personnel. The Information Technology personnel are being granted the access either for configuration tasks or at regular intervals for the monitoring of the servers and networks
- Constant updating of the antivirus software that is in use for protecting the personal computers in use by the Company's personnel. The update is performed hourly to ensure maximum security and protection.
- Regular updates of the servers thus ensuring the maximum security of the data stored. The maximum security is essential for protection of the data in terms of both malicious attacks and the loss of data due to 'Significant Business Interruptions'. The updates are both operating system and application updates.
- Passwords are provided to users of the different software in use by the Company. It is the responsibility of the personnel for all transactions/actions made while their password is in use. For security reasons no user is allowed to access the server/network with another user's account and password.
- Conduct thorough tests to any version change of the Company's Gaming Platform in a staging environment prior to updating the production servers thus highlighting any problems before updating the production version.
- Check on a daily basis the telephone system log and a system backup regularly. In case of any failure of the system, the Company has agreements with various telecommunications providers that will provide the Company with temporary back up lines in case of failure.

b) Information Technology Backup

The Company shall proceed in the storing of electronic backups, in order to ensure that all important information can be retrieved as requested, and to prevent loss of data in situations of interruptions. The Company shall have in place procedures for incremental daily backups and weekly and monthly backups.

The following actions shall be taken by the Company:

- On a daily basis provide backup on all servers and other important personal computers (Senior Management).
- Keep backups on files stored on other external storage device
- On a weekly basis back up all data and proceed in storing them outside the Company's premises
- Duplicate a Real server on the 'slave' Real server for creating a back up of all the information held on the Server in real time

c) Building Security

The Department through an electronic access control system shall ensure that business security is in place as required by legal requirements that all Company's premises are controlled, monitored and are secure. Access to the buildings is only through access cards provided to all relevant people and it is their responsibility for the safeguarding of the access cards.