

CENTRUM
Know Your Customer / Anti-Money Laundering /
Prevention of Terrorist Financing / Prevention of
Financing Proliferation / Player Protection
Policies Manual



CENTRUM GLOBAL B V

VERSION 2025-01

CENTRUM GLOBAL B V

Two blue ink signatures are shown, one on the left and one on the right, both written in a cursive style.

Signed by e-Management N.V. (Managing Director)

TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	Background and Approach	5
1.2	Business Model and implication for AML/PTF/PFP Policy	6
1.3	Overall Policy	6
1.4	MLRO and DMLRO	6
1.4.1	Appointment to role	6
1.4.2	Procedures will be maintained to ensure the following:	7
1.4.3	Responsibilities	7
1.4.4	Provision of Education and Training	8
1.4.5	Regime and Culture	8
1.4.6	Review of effectiveness	8
1.5	The RISK BASED Approach	8
1.6	What is Money Laundering?	9
1.7	What is Financing of Terrorism?	9
1.8	What is Financing of Proliferation of weapons?	10
2	RISK ASSESSMENT	11
2.1	Business Risk Assessment	11
2.2	Player Risk Assessment	12
2.2.1	Nature of Participants	12
2.2.2	Status of Participants	12
2.2.3	Location of Participants	13
2.2.4	Amount of funds being transacted	13
2.2.5	Nature and frequency of transactions	14
2.2.6	Player Risk Matrix	14
3	PLAYER IDENTIFICATION AND CORE KYC	15
3.1	General:	15
3.2	Anonymous Accounts	15
3.3	Evidence of identity for participants	15
3.4	Enhanced Participant due diligence	16
3.5	KYC Matrix	18
3.6	On-going Monitoring of Participants	18
3.7	On-going Monitoring of transactions	19

4	RECORD KEEPING AND RETRIEVAL OF RECORDS	20
4.1	Record of Transactions	20
4.2	Retention of Records	20
4.3	Register of Money Laundering enquiries and reports	21
5	INTERNAL PROCEDURES INCLUDING THE REPORTING OF SUSPICIOUS TRANSACTIONS, BOTH INTERNAL AND EXTERNAL	23
5.1	Internal suspicious activity reporting	23
5.2	Reporting and “active” business	23
5.3	External suspicious activity reporting	23
5.4	External Sanctions Reporting	24
6	WHISTLEBLOWING POLICY	25
6.1	Whistleblowing	25
6.2	Whistleblowing Steps	25
7	RESPONSIBLE GAMING POLICY	26
7.1	Responsible Gaming Policy	26
7.2	Application of Responsible Gaming in a Non-Retail Context	26
8	PLAYERS COMPLAINTS POLICY	27
8.1	Players Complaints Policy Aim	27
8.2	Key Actions Required by CENTRUM	27
8.3	Valid Reasons for Complaint	27
8.4	Complaint Submission Process	27
8.5	Complaint Resolution	28
8.6	Complaint Acknowledgement	28
8.7	Complaint Resolution Timeline	28
8.8	Alternative Dispute Resolution (ADR)	28
8.9	Authority Escalation	28
8.10	Contact Points for Complaints	28
8.11	Record-Keeping	29

8.12	Regulatory Reporting	29
8.13	Visibility in Terms and Conditions	29
9	ALTERNATIVE DISPUTE RESOLUTION POLICY	30
9.1	Alternative Dispute Resolution Policy Aim	30
9.2	Obligation to Offer ADR	30
9.3	Process Requirements	30
9.4	Operator Non-Participation	30
9.5	Binding Nature of ADR Decisions	30
9.6	Transparency and Disclosures	30
9.7	Recordkeeping and Communications	31
9.8	Reporting and Monitoring	31
9.9	Continuity of ADR Service	31
10	STAFF RECRUITMENT, EDUCATION, TRAINING AND DEVELOPMENT	32
10.1	Importance for AML/PTF/PFP risks	32
10.2	The importance of staff in ML prevention	32
10.3	Human Resources risk factors in ML prevention	32
10.4	Integrity	32
10.5	Staff Recruitment	32
10.6	Staff Knowledge, Training and Awareness	33
10.7	Compliance with company policies and procedures	33
10.8	Technological Developments	33
11	POLICY REVIEW / AUDIT AND INDEPENDENT TESTING	35
11.1	Policy Review and Audit	35
11.2	Independent Testing and Software Certification	35
12	VERSION CONTROL	36
13	APPENDICES	37
13.1	Appendix A – Suspicious Transaction Report	37

1 Introduction

1.1 Background and Approach

The objective of this manual is to provide a high-level assessment of the operations and services provided by Centrum Global B V and the risks that they may facilitate money laundering or the financing of terrorism or financing of the proliferation of weapons and to set out the policies, procedures, systems and controls necessary for Centrum Global B V to meet its obligations to prevent these from happening.

Centrum Global B V's approach is based upon the well accepted international standards and, amongst other policies of the Curaçao jurisdiction, some of which, are listed below:

- National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92)
- National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).
- National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282)
- National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283),
- Sanctions National Ordinance (N.G. 2014 no. 55)
- National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73)
- Article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92) and;
- Article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54).

Together referred to as "the codes" in relation to the detection and prevention of money laundering and terrorist financing.

The procedures that are appropriate for the purpose of forestalling and preventing money laundering include:

- Identification
- Record keeping
- Internal procedures including the reporting of suspicious transactions, both internal and external
- Staff education, training and development

Centrum Global B V is required to assess its Anti-Money Laundering (AML) / Prevention of Terrorist Financing (PTF) risks and implement appropriate measures in respect of the above based on its assessment. This manual sets out how management achieve this.

Centrum Global B V intends to always remain in full compliance of all the Curacao Gaming Authority (CGA) recommendations that are applicable to the organisation.

1.2 Business Model and implication for AML/PTF/PFP Policy

Centrum Global B V has always and will always be focussed on the following business model:

- No ONLINE Betting is available
- No RETAIL Betting Websites
- Only High Volume, Algorithmic, Mathematical Based Professional Play is catered for
- All players are carefully vetted and signed agreements are entered into with each player
- Only bet on PARI MUTUEL Animal (Horses, including Trotting, or Greyhounds) racing events
- No FIXED ODDS or CASINO STYLE GAMES or POKER or iGAMING or LOTTERIES are available via CENTRUM GLOBAL B V
- Not a single retail player will ever be allowed to become a client of CENTRUM GLOBAL B V.

As such, all our related KYC / AML / PTF / PFP / PLAYER policies are focussed on this type of player.

1.3 Overall Policy

It is Centrum Global B V's policy that it has statutory and regulatory obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

Positive management action will be exercised to minimise the risk of the company's services and gaming activities being abused for the purposes of laundering funds associated with criminal activity, as defined by the relevant legislation.

Centrum Global B V will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the relevant authorities and in accordance with regulations.

1.4 MLRO and DMLRO

1.4.1 Appointment to role

Centrum Global B V shall always have an appointed Money Laundering Reporting Officer (MLRO) and at least one Deputy (DMLRO).

The appointed MLRO will be sufficiently senior within the company and will have the right of direct access to the Directors of the company.

The MLRO and DMLRO will have unfettered access to all reports, transaction histories, complaints and audit trails.

The following – at the time of writing are the names of those fulfilling these roles.

Money Laundering Reporting Officer

CHRISTIAN HEAP

Deputy Money Laundering Reporting Officer(s)

DENNIS VERRIOS / RACHNA AHUJA

1.4.2 Procedures will be maintained to ensure the following:

- All persons conducting business with the company are properly identified, that their identity is verified where appropriate and sufficient information is gathered and recorded to permit the company to “know its client” and predict the expected pattern of business.
- Potential new participants that do not appear to be legitimate are declined and where there is suspicion relating to criminal conduct on the part of a declined participant such suspicion is reported to the Money Laundering Reporting Officer (MLRO) or the Deputy Money Laundering Reporting Officer (DMLRO).
- Established participants activities are regularly monitored to ensure that they fit the customer’s profile, especially in respect of large or abnormal transactions.
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- All suspicions are reported promptly to the MLRO or the DMLRO.
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation
- That the company’s vigilance systems are implemented and regularly monitored.

1.4.3 Responsibilities

Centrum Global B V’s management is responsible for:

- The day-to-day compliance with anti-money laundering obligations within the areas of the company for which they are responsible.
- Ensuring that the MLRO or DMLRO is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the MLRO or DMLRO with the appropriate resources to fulfil the function effectively.
- Ensuring that the MLRO or DMLRO has complete autonomy in the suspicious activity report evaluation process and unfettered access to information necessary to carry out that process.
- The Directors and MLRO will ensure that he/she is provided with or has access to the necessary resources to keep up to date with new money laundering requirements and developments.

The MLRO is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the company to all external agencies and any other third-party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Undertaking the internal review of all suspicions and determining whether such suspicions have substance and require disclosure to FIU.
- All contact between the company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the MLRO or DMLRO all knowledge or suspicions of money laundering.

- Complying fully with all money laundering procedures in respect of client identification, client monitoring, record keeping, vigilance and reporting.

1.4.4 Provision of Education and Training

All members of management and staff will receive regular briefings and/or training as and when required.

1.4.5 Regime and Culture

Detailed and comprehensive policy and procedures are not sufficient to forestall the facilitation of money laundering. If the culture of an organisation is to circumvent or ignore the rules, then they will be ineffective.

It is the policy of the company's directors and senior management to encourage a compliance culture by:

- Demonstrating support for compliance with these procedures and with sound corporate ethics
- Providing support for staff in their AML/PTF/PFP efforts
- Demonstrating support for the MLRO
- Demonstrating no tolerance of clients and other external parties who are not transparent or are not cooperative in AML/PTF/PFP efforts
- Encouraging risk awareness in staff
- Encouraging a spirit of compliance
- Taking appropriate action in respect of breaches
- Encouraging the raising of concerns by staff at all levels
- Providing the necessary resources for proper application of procedures and to address concerns

1.4.6 Review of effectiveness

Management will review and assess the culture within the company and the effect of human factors on the effectiveness of procedures as part of its risk review.

1.5 The RISK BASED Approach

An anti-money laundering compliance program is an essential component CENTRUM GLOBAL's compliance program. The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

Based on the CGA Recommendations, we are required to apply a Risk-based Approach when designing policies, procedures and controls to combat money laundering, financing of terrorism and financing of proliferation of weapons. By adopting a Risk-based Approach, it is possible for CENTRUM GLOBAL B V to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified. When drawing up the antimoney laundering compliance program, a casino takes a risk-based approach. That means the higher the risk, the more measures the casino has to take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower it may take simplified measures, provided that this is consistent with the country's assessment of its money laundering / financing of terrorism risks.

Applying Risk-based Approach means that a casino has to:

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

1.6 What is Money Laundering?

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;

Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;

Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

Most of the people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for money laundering such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

1.7 What is Financing of Terrorism?

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations.

A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards.

While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

1.8 What is Financing of Proliferation of weapons?

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

2 Risk Assessment

2.1 Business Risk Assessment

As part of the companies regulated approach to AML/PTF/PFP risk the following assessment has been conducted in order to adopt a risk-based approach to compliance with customer due diligence, both at the point of registration and in relation to on-going monitoring of clients.

The following outlines an analysis of the AML risks faced by the Company. This is reviewed and updated on a regular basis, at least annually:

Risk Factor	Comment	Risk
Public Profile of the Company?	Centrum is a private network and therefore has a negligible public presence.	LOW
Customer Profile?	These are well known businesses or individuals within the industry in which Centrum operates. All key individuals or management members (in the case of companies) are highly professional and often exposed directly to the markets in which Centrum operates for face-to-face meetings. Centrum has no intention of keeping its customers away from the markets but rather promotes a culture of open discussion.	MEDIUM
Staff knowledge of players?	All are known individually by the key management of Centrum. The customers (or targeted customers) are very well known and limited in number. The key members of the Centrum operation have known these customers and their key personnel for many years.	LOW
Existence of PEPs?	Centrum has not and has no intention of establishing relationships with any PEPs. Systematic checks are undertaken prior to the commencement of a relationship in order to ascertain any PEP exposure.	LOW
Non face-to-face customers?	As per the customer profile all customers are known to the business.	LOW
Use of vulnerable payment methods?	All transactions are undertaken through direct banking relationships with customers through suitably regulated banking providers.	LOW
Is customer's source of wealth exposed to significant amounts of cash?	Significant source of wealth checks are undertaken prior to commencement of any customer relationship. Any exposure to cash would be identified and managed appropriately.	MEDIUM
Likelihood of customers being unable to evidence source of funds/source of wealth?	The sector that Centrum supports is easily researchable. They are well known operators at the very top of their profession and as such their history, and rise to positions of wealth are all well documented.	LOW
Use of 3 rd party accounts?	Due Diligence is always conducted as a matter of course to connect the bank account to the account holder or their approved Funding parties (related).	LOW
Profile of transactions?	In order to facilitate the high velocity of bets undertaken by the customer the transaction values with Centrum will be high and on a high frequency basis.	HIGH
Monitoring Process?	Monitoring of wagering activity is a daily process. Firstly, all wagering is conducted on a funded account basis. All wagering is ultimately tied back to a bank transaction into the customer's account. If market conditions suggest that wagering is to be unusually high then there is always communication between Centrum Operations and the customer wagering team. The reason for this is that systems need to be checked to eliminate any volume limits that may be set. Market reports are processed for the previous day each morning and those are passed in front of three resources before being released. Mathematical customers betting pattern follow a regular pattern, so any movement away from the pattern is easily picked up. Should this occur, there are internal conversations paths before the customer is contacted for clarification. If there was ever an explanation and a combined result that did not match the pattern or the explanation, then this would amount to 'suspicious activity' and the prescriber procedures followed.	LOW

This assessment indicates that the business presents an overall low to medium risk of money laundering. Although the deposit values are high all clients are known to the business and undergo applicable risk based CDD prior to acceptance by the business. All client funds are presented through the banking system, and all activity is recorded. This goes some way to mitigating the likelihood of any customer using the business to launder criminal property or spend the proceeds of criminal activity through the Company's systems.

2.2 Player Risk Assessment

Centrum Global B V must consider the AML/PTF/PFP risks associated with its service offering and adopt a risk-based approach when considering the requirements for:

- Identity of participants
- Evidence of identity
- Enhanced participant due diligence

The business undertaken by the company and management's assessment of its inherent money laundering/terrorist financing risk has been considered as follows:

The major factors that may highlight increased or decreased potential risk are:

2.2.1 Nature of Participants

Business Participants are considered by the company to represent a greater risk to the company from an AML/PTF/PFP risk, than an individual participant.

It is management's considered view that a Business Participant transacting with the company in what may be considered a normal manner represents only a minimal enhanced risk of money laundering or terrorist financing.

Nevertheless, the risk is enhanced and as such, satisfactory evidence of the nature and identity of the Business Participant is considered by Management to be essential prior to the business relationship being entered. This is considered in later sections.

2.2.2 Status of Participants

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting. It is management's considered view that a PEP transacting with the company will not be allowed at all unless a very specific case is presented for doing so.

Screening is undertaken to identify PEP or Sanctioned Individuals at the onset of the participant relationship and on an ongoing basis (at least annually) through the monitoring procedure.

2.2.3 Location of Participants

A participant located in a jurisdiction which is not Financial Action Task Force (FATF) compliant, may generally be considered to represent a potential risk of money laundering or terrorist financing activity. However, it is management's considered opinion that an individual transacting with the company in what may be considered a normal manner, but from such a territory, represents only a minimal enhanced risk of money laundering or terrorist financing.

Whilst the above factors are considered when determining the identification requirements at registration, Management considers that other factors, when combined with the above, create heightened risk of on-going money laundering or terrorist financing activity. These contributory factors include but are not limited to:

- Amount of funds being transacted
- Nature and frequency of transactions

To determine the participant risk, these factors will be considered on a case-by-case basis.

A monthly review is conducted across all registered participant jurisdictions. The review monitors both AML/PTF/PFP and commercial consideration. The monthly overview of the jurisdictions takes place to check that players have not been accepted from FATF closed or deficient jurisdictions. This review is monitored and reviewed by senior management including the MLRO.

2.2.4 Amount of funds being transacted

Generally, all CENTRUM GLOBAL B V's players will deposit large values. So, the following condition is more based on expected "norms". These will be monitored, but more importantly to us is suspicious activities with deposits or requested withdrawals.

NORMAL "RETAIL" POLICY – Keep a watchful eye on all deposits

The regulatory environment around retail organisations is for any funds transacted over CG 4,000 or aggregate in excess of CG 4,000 in any day (qualifying payments), there is an enhanced risk of money laundering or terrorist financing activities and additional identity checks are undertaken).

However, this value is not deemed to apply to CENTRUM GLOBAL B Vs Risk Based approach given the nature of its business model.

Indeed, the average Deposit value for CENTRUM GLOBAL B V is in excess of CG 250,000. However, due to the winning nature of the professional player – each player generally does not deposit often as they only need to start their "bank" off with an amount and then generally win over regular periods.

LARGE DEPOSIT POLICY

On its own, the risk associated with large deposits may not be overly significant. However, when combined with irregular or unusual account activity or with the PEP status or location of the participant, the risk may be significantly enhanced.

Centrum Global B V maintains a watchful eye on all DEPOSITS including ML actions such as smurfing and other methodologies.

2.2.5 Nature and frequency of transactions

Where an individual is making regular deposits and betting transactions there is considered only minimal potential risk of money laundering or terrorist financing. Irregular patterns of activity or regular deposits and withdrawals with limited betting transactions may highlight enhanced risk.

The procedures detailed in the following pages address both the requirement to identify participants and to gather evidence verifying their identity but also to monitor on-going activity to determine a change in the risk profile of the participant.

2.2.6 Player Risk Matrix

Following an in-depth review of the preceding factors by the Company's senior management the following matrix details the Company's AML/PTF/PFP approach to player risk.

RISK RATING



CLIENT ID Number: _____

Rating: _____

Reason for rating: _____

e.g.: Individual, personally known, trading levels, known to management and location etc

R i s k R a t i n g	No Account	Complex business participants with beneficial owner who is senior PEP	Closed jurisdiction	Cash	n/a
	High Enhanced	PEP or have any close association/relationship with PEP. Any other relevant matters and warning notices issued	PEP / Sanctioned List	Bank transfer from unapproved Vehicle	\$10,000,000 +
	High	Adverse publicity or unlicensed business player	Regulator non-compliant	Bank transfer from SPV	\$5m+
	Medium	Business Participants	Regulator Compliant	Bank transfer from Associated Company or KYCd 3 rd Party	\$2m to \$5m
	Low	Individuals or licensed business participant	Place of Licence or business	Bank transfer from participant	\$0 - \$2m
	Nature		Jurisdiction (to include location of business, identity and origination of funds for both business participants and individuals);	Source of Funds from Deposit	Transaction Size (Cumulative Daily Stake)

Following the risk assessment participants will be identified as either low, medium, high or high enhanced. The relevant level of customer due diligence will then be applied to each participant's account and reviewed on an on-going basis as part of the monitoring procedure.

Sanction and PEP checking will be part of the Company's initial risk assessment at the beginning of the relationship and will take place daily following acceptance of the participant. The NAMESCAN system is utilised for this purpose. PEPs are automatically classified as high risk.

PEPs or a person from a high-risk jurisdiction will be subject to enhanced customer due diligence and on-going monitoring.

3 Player Identification and Core KYC

3.1 General:

The company does not facilitate any gambling activity or the depositing of funds for this purpose unless the intended participant has:

- Registered with the company and
- has created an account with the company and
- has confirmed their acceptance of the terms and conditions and
- provided the applicable due diligence.

To register, a player must first complete a company application form.

No player under the age of 18 can register with the company. If their age is below 18, they will not be accepted as a participant.

Known problem gamblers will be excluded from registration as will gamblers who have previously been excluded.

Records will be maintained by Centrum Global B V's administration of all current, attempted and past registrations.

Upon provision of all documentation and confirmation of agreement to the terms and conditions, an email will be sent to the registered user at the email address provided. Registration will not take place if all documents are not provided and no monies can be deposited with the company until the account has been activated.

3.2 Anonymous Accounts

Players will not be able to register with fictitious names or anonymous accounts as we have no website or anonymous registrations.

3.3 Evidence of identity for participants

Centrum Global B V are aware that payments made to participants that exceed Euro 3000 or payments which taken cumulatively within a 30-day period exceed Euro 3000 are classified in the Codes as qualifying payments and as such trigger the requirement for evidence to be gathered confirming the registered participants' identity. However, it is anticipated that all customers will exceed this threshold during the early stages of the relationship therefore the company obtains due diligence prior to the participant being accepted as a player.

The documentation requested prior to accepting the participant are as follows:

a) Verification of identity:

The following are acceptable identity documents:

- A passport
- A national ID or armed forces ID card
- A full driving licence

To be acceptable identity documents must be:

- A good clear copy, plainly legible,
- Unexpired at the date of receipt,
- Bear a photo of the holder, and
- Signed by the holder (if appropriate).

b) Verification of address:

- A recent account statement (i.e. no more than 3 months old) from a recognised bank, building society or credit card company or the most recent mortgage statement from a recognised lender or a validated Lease agreement.
- An unexpired photographic driving licence or national identity card containing current residential address if the document has not been used to verify identity.
- A recent rates, council tax or utility bill (recent in respect of utility bills is considered to be for the last quarter i.e. no more than 3 months old). Mobile telephone bills are not acceptable as evidence of address under any circumstances.
- Correspondence from an official independent source such as a central or local government department or agency.

Only upon receipt of the documents to a satisfactory standard will management authorise the activation of the account and permit the participant access to the system.

The account will be marked as having passed basic customer due diligence.

The Administration team will also consider whether a suspicious transaction report should be made to the MLRO or DMLRO. The factors that may influence that decision are:

- If the required documents are not received and the monies and account remain suspended.
- The transaction history. If none or very few bets have been placed and a withdrawal of deposited funds is being requested, this may lead the Administration team to consider the transaction suspicious
- If bets are being placed regularly and monies won this should not normally raise suspicions
- If a single bet is placed and large monies are won, suspicions may be raised as to the integrity of the system

If suspicious activity is considered a possibility a suspicious transaction report will be lodged in accordance with the procedures set out in this document.

3.4 Enhanced Participant due diligence

In certain cases, highlighted by the risk assessment (see section 3), management may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the company. Participants who pose an additional risk will be marked within the administrative system and a report of their transactions made available to the MLRO.

Enhanced due diligence will consist of the following:

- requirement of additional identification data
- Consideration as to whether this data needs to be certified
- Establish the source of funds
- Establish the source of wealth

- Flag the participant for ongoing monitoring
- Consideration of a 3rd party background check
- Open source checks

A participant who poses higher risk may be:

- a head of state, head of government, minister or deputy or assistant minister;
- a senior government official;
- a member of parliament;
- a senior politician;
- an important political party official;
- a senior judicial official;
- a member of a court of auditors or the board of a central bank;
- an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- a high-ranking officer in an armed force;
- a senior member of an administrative, management or supervisory body of a State-owned enterprise;
- a senior official of an international entity or organisation; and
- an honorary consul

Any family members of a person mentioned above, including a spouse or equivalent, child or the spouse or partner of a child, brother or sister (including a half-brother or half-sister), parent, parent-in-law, grandparent or a grandchild.

- Any close associate of a person mentioned above including:
- Any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;
- Any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;
- Any natural person who is known to be the beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary;
- Any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

Or a person;

- A resident in a country which the company has reason to believe does not apply or insufficiently applies the FATF recommendations.
- Meets the EDD requirements on the risk matrix due to their level of transactions or method of deposit.
- Any persons that are the subject of any warnings or notices issued by the regulator will be considered a higher risk.

Business Participants are also considered to represent an enhanced risk. Prior to relationships with Business Participants being entered into, enhanced due diligence will be obtained. This will include:

- Verification of the identity and address of the shareholders (representing in excess of 20% of the total shares issued) and all directors and controllers of the business participant
- A copy of the company's certificate of incorporation and memorandum and articles of association
- Copy of a board resolution authorising certain individuals to act on behalf of the company

- Confirmation of the geographical sphere of the company's operations
- Nature of its activities
- Name of Regulator (if appropriate)

Based on the risk assessment, and on each individual case, management will decide whether a company search is required and in what form additional due diligence is required. Additional due diligence will include:

- World-Check is an independent online database containing names and details of individuals that may be considered a heightened risk to the company. Examples of individuals featured on the World-Check database include Politically Exposed Persons (PEPs), prominent public figures or persons known or suspected to be involved in financial crime
- Consideration by the company as to whether additional aspects of the participants identity should be verified – perhaps through the certification/notarisation of identity and address verification, securing of bank references etc.
- ~~Consideration by the company as to whether information is required on the source of funds and the source of wealth/background of the participant~~

3.5 KYC Matrix

Following an in-depth review of the preceding factors by the Company's senior management the following matrix details the customer due diligence requirements:

3.6 On-going Monitoring of Participants

KYC REQUIRED

CLIENT ID Number: _____

Rating: _____



3 rd Party Background Check	Enhanced					X
	Basic or knowledge statement from CENTRUM				IF POSSIBLE	IF POSSIBLE
	PEP & Sanction Screening	X	X	X	X	X
	Open Source Checks	X	X	X	X	X
ID and Address Verification	Utility Specific		X	X		CERTIFIED
	Basic – 100pt Inc. Photo ID and 2 Address Documents	X	X	X		CERTIFIED
	Source of Wealth	X	X	X		CORROBORATED
		Low	Medium	High		High Enhanced

Participants (including business participants) are monitored on a daily basis but at least annually Centrum Global B V reviews the company's identification and risk matrix procedures to ensure that the participants CDD and risk ratings are up to date and in line with their transactions.

3.7 On-going Monitoring of transactions

The monitoring of wagering activity by the company is a three-step daily process.

Files are received from the host market and are integrated into the company's reporting system. Activity reports are created by market, customer, bet type and by track.

The above granularity enables the company to take a granular look at the activity of every customer, from that the company can determine a pattern of betting that becomes the norm.

Customers bet following various methodologies, they are not swayed by 'feelings or hunches' and therefore the patterns of activity are particularly regular.

Stage 1 monitoring;

All activity is first reviewed by the Financial Reporting team prior to reports being released.

Stage 2 monitoring;

Following report release, Operations will review the numbers in order to determine the account status of a customer for future wagering activity. From this any significant variation in pattern becomes instantly clear, as the expected balance will be vastly different from the actual wagering balance.

Stage 3 monitoring;

The Account Manager reviews the numbers for two reasons. Firstly, to ensure that, like Operations, there is enough wagering balance to perform the next day's activity, but also to ensure that the pattern of wagering would not alarm the market into which the wagers are being placed.

Any unexpected activity can often be explained by such things as additional tracks on which to bet being available, or on unusually high jackpots available from the host market, but any suspicious activity that cannot be explained will then follow the Suspicious Activity Procedure for further investigation.

If during the course of daily monitoring it is noted that a player's profile has altered in a way that would alter their risk level an immediate review would be undertaken to ensure that all CDD criteria for the new risk level is met. Should any further documents or information be required the participant will be contacted with a request to provide such within a timely manner.

4 Record keeping and retrieval of records

4.1 Record of Transactions

Centrum Global B V will maintain appropriate records of all participants and their associated transactions. The Island based Operations Manager and MLRO have unfettered access to all records (other than those which are stored in an encrypted or hashed form) and reporting through the back-office computer system. All records and audit trails can be accessed by them and reported in hard copy format without delay and within 7 days of any request being made.

- Identification and verification of identify

The Operations Manager and MLRO will always retain access to the back-office computer system which holds the registration details of all participants. Such records can be accessed without delay via bespoke reports accessed/generated by the back-office system.

The MLRO can retrieve all identity verification that has been collated on those considered to pose a higher risk or those who have been subject to qualifying payments. Hard copies can be retrieved on request.

- Deposits, Withdrawals, Bets, Dividend Payments

All financial transactions are recorded against the participant within the back-office system and are reconciled against banking records provided by the bank. This includes the name of the participant or unique identity number, the amount and nature of the transaction, the date of the transaction, the source or recipient of the funds and the nature of the financial transaction.

All financial transactions are maintained in a system audit log which is available to the MLRO and Operations Manager upon request.

Each transaction is recorded in the database of the website with a specific reference. Transactions are sorted in the back-office using the same reference pattern and can be scrutinised by the Operations Manager and MLRO by date, participant or nature of the transaction.

4.2 Retention of Records

Records will be maintained in a secure and accessible form: Secure backups of all data are made daily.

Records include:

- all registration details
- identification verification
- enhanced due diligence
- suspended accounts and reason for suspension
- closed accounts
- suspicious transaction reports
- financial transactions – deposits, bets made, withdrawals, Dividend payments
- bets placed

- complaints and responses
- audit trails
- accounting and bookkeeping records
- bank reconciliations
- Customer Service electronic correspondence records

Records associated with a participant (including all identification records and the financial transactions made by them) are maintained for a period of 6 years after the date of closure of the participant's account or the date of the last transaction.

The MLRO or DMLRO logs any Participants who have been the subject of a suspicious transaction report on the computer system. Records associated with such participants will be maintained until such time as the MLRO agrees to them being destroyed. In cases where an ongoing investigation is being conducted, the MLRO will retain the records until such time (but in any case, for at least 6 years) as the investigating FIU officer confirms that the records are no longer required.

4.3 Register of Money Laundering enquiries and reports

The MLRO maintains a register separately from other records associated with the company which details:

- Enquiries made to Centrum Global B V by law enforcement or other officials acting under powers provided by the Money Laundering and Terrorist Financing Requirements

This register contains:

- The nature and date of the enquiry
- The name of the enquiring officer and enforcement agency
- The powers being exercised
- Details of the participant
- Details of the transaction
- Outcome of enquiry (if known)

- All reports made to the relevant regulatory body regarding suspicious transactions

This register contains:

- The nature and date of the report including details of the participant and the transaction
- The name of the person making the report
- The name and agency to whom the report is made
- Information about the transaction which is sufficient to identify the relevant papers
- Details of the acknowledgement of receipt of report provided by the Financial Intelligence Unit
- Outcome of enquiry (if known)

- All reports made to the MLRO or DMLRO by Centrum Global B V employees

This register contains:

- The nature and date of the report including details of the participant and the transaction
- The name of the person making the report

- Information about the transaction which is sufficient to identify the relevant papers
- Details of the acknowledgement of receipt of report provided by the MLRO or DMLRO
- Outcome of the report

5 Internal procedures including the reporting of suspicious transactions, both internal and external

5.1 Internal suspicious activity reporting

Suspicious must be reported to the MLRO or DMLRO as soon as reasonably practical using the attached form, as per Appendix 13.1. The form is also available on request from the MLRO or DMLRO. The case may be discussed initially with the MLRO or DMLRO, but a telephone discussion is not a substitute for formal notification using the appropriate form.

It is important that the form is used as this properly documents the report itself and ensures that all relevant information is included. For this reason, it is important that all parts of the form are completed.

Receipt of the report will be acknowledged by the MLRO or DMLRO.

It is not necessary for the person making the report to include their name on it. However, if an acknowledgement is required the person making the report will need to identify themselves to the MLRO in some other way, such as by providing a covering memo.

Once an initial report has been submitted the person should continue to submit reports where further suspicious activity takes place, or if there are developments in respect of the matter originally reported.

5.2 Reporting and “active” business

Where a suspicion is reported in respect of a transaction that has not taken place or an activity that has not commenced this fact should be made clear to the MLRO or DMLRO. If the person submitting the report is involved with the transaction or activity they should not do anything further until advised that they can do so by the MLRO or DMLRO.

The MLRO and DMLRO in conjunction with the Directors will manage the process of ensuring that the transaction may proceed, including obtaining Financial Crime Unit clearance if appropriate.

5.3 External suspicious activity reporting

The MLRO and DMLRO have full access to information and records of the company that the Directors consider necessary to evaluate internal reports received. They will document the evaluation process and the reasons for conclusions reached.

If after completing the evaluation process the MLRO or DMLRO considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO or DMLRO are responsible for:

- Submitting the necessary information to the relevant regulatory Financial Intelligence Unit (“FIU”)
- Recording the disclosure in the register of disclosures
- Dealing with subsequent production or account monitoring orders, if there are any.

5.4 External Sanctions Reporting

Where a participant is flagged as being on a sanctions list, specifically the EU or UN sanctions list, the MLRO will report such to the regulator. Such accounts are frozen and no money must leave the Company's platform. This will also prompt consideration being given to whether there is a suspicion of money laundering or terrorist financing and a requirement to file a suspicious activity report to the FIU in accordance with the relevant section of this document.

6 Whistleblowing Policy

6.1 Whistleblowing

If, in the course of employment, an employee becomes aware of information which they reasonably believe tends to show one or more of the following, they must use Centrum Global B V disclosure procedure set out in the Whistleblowing Steps:

- That a criminal offence has been committed is being committed or is likely to be committed.
- That a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject.
- That a miscarriage of justice that has occurred, is occurring, or is likely to occur.
- That the health or safety of any individual has been, is being, or is likely to be endangered.
- That the environment, has been, is being, or is likely to be damaged.
- That information tending to show any of the above, is being, or is likely to be deliberately concealed.
- That the business or any associated person has been, is being, or is likely to be receiving or offering bribes.
- That any foreign official has been, is being, or is likely to be bribed or offered facilitation payment by the company or any associated person.

6.2 Whistleblowing Steps

If an employee or associate of the organisation notes any of these, they should immediately report to the MLRO if appropriate, else to the Director of the organisation if appropriate or direct to the appropriate department in the Curacao government. The employee or associate should do so without fear of repercussions from CENTRUM GLOBAL B V.

7 Responsible Gaming Policy

7.1 Responsible Gaming Policy

CENTRUM GLOBAL B V is committed to fostering a safe, transparent, and fair betting environment to its customers.

Under the requirements of the CGA general retail operators must allow for:

- Clear Responsible Gaming policy that is easily available to the players.
- Provision of Responsible Gaming tools and information resources to players.
- Monitoring mechanisms must be in place to detect and address problematic gambling behaviour.
- Compliance with all regulatory reporting and auditing obligations.

However, CENTRUM GLOBAL B V operates what is known to the CGA as a “**Non-Retail Model**”

And as agreed with the CGA, CENTRUM GLOBAL B V does not generally need to apply a specific Responsible Gaming Policy to non-retail gaming and betting including but not limited to professional players or syndicates.

In CENTRUM GLOBAL BV's business, a general Responsible Gaming principles apply in line with such business models.

7.2 Application of Responsible Gaming in a Non-Retail Context

While CENTRUM GLOBAL B.V. does not cater to retail consumers and does not offer direct-to-public services, it recognises the importance of upholding the integrity and social responsibility expectations of the Curaçao Gaming Authority.

CENTRUM GLOBAL B.V. therefore adopts the following principles to meet the spirit of Responsible Gaming within a professional betting environment. CENTRUM GLOBAL B.V. will:

- Ensure that all counterparties are **fully verified professional entities or individuals**, with appropriate due diligence conducted to assess suitability and experience.
- Require all parties to **acknowledge the high-risk nature of wagering activities**, and that their involvement is commercial, professional, and strategic.
- Maintain contractual provisions that **clearly state the professional nature of play**, and the expectation that players are not vulnerable individuals or members of the general public.
- Monitor for any unexpected activity that may indicate non-professional involvement and take immediate steps to restrict or suspend such activity if detected.
- Maintain clear internal policies regarding the **exclusion of any retail or non-professional customers**, and commit to immediately notifying the CGA should any such activity be identified.

This approach ensures that CENTRUM GLOBAL B.V. operates responsibly within the **non-retail exemptions** afforded under CGA policy, while still upholding the principles of accountability, transparency, and professional integrity.

8 Players Complaints Policy

8.1 Players Complaints Policy Aim

The aim of this policy is to ensure all player complaints are managed transparently, fairly, and efficiently, in line with Article 5.3 of the National Ordinance on Games of Chance (LOK), including access to independent Alternative Dispute Resolution (ADR).

8.2 Key Actions Required by CENTRUM

CENTRUM GLOBAL B V will always:

- Maintain a clear, accessible complaint process provided to each of its customers.
- Respond to all complaints within set timelines.
- Offer free access to an approved ADR provider.
- Maintain complaint logs and submit regular reports to the CGA.
- Display complaint information in the Terms and Conditions within its agreements.

8.3 Valid Reasons for Complaint

Players may raise complaints about:

1. Deposit issues
2. Withdrawal issues
3. Bonus terms and conditions
4. Account closures or restrictions
5. Alleged errors or unfairness in game outcomes
6. Responsible gaming issues
7. Treatment of player balances
8. KYC and Verification
9. Data Protection
10. Technical or Software issues
11. AML concerns
12. Fraudulent markets/races
13. Fraudulent practices
14. License or regulation

8.4 Complaint Submission Process

CENTRUM GLOBAL B V will ensure the following processes are adhered to:

- Players can submit complaints **free of charge** within **six months** of the event (or its resolution in ante-post betting).
- Complaints must be submitted through an email to the client's account manager
- The email must include player identity, account number, date, description of the issue, language preference (English or local), and supporting documents.

8.5 Complaint Resolution

CENTRUM GLOBAL B V will ensure the following processes are adhered to:

- Complaints involving responsible gaming are prioritised.
- CENTRUM GLOBAL B V must aim to resolve complaints within **5 business days**.
- If more time is needed, the player must be notified; the delay **must not exceed 2 weeks**.

8.6 Complaint Acknowledgement

Within **one week**, CENTRUM GLOBAL B V must:

1. Confirm receipt of the complaint.
2. Outline the processing procedure.
3. Provide an estimated timeline for resolution.

8.7 Complaint Resolution Timeline

CENTRUM GLOBAL B V will ensure that it adheres to the following timeline:

- It has four weeks to respond, extendable once by another four weeks with written notice.
- The final response must be in writing and include either:
 - » A reasoned outcome with evidence; or
 - » Reasons for not handling the complaint, including any request for further information.

8.8 Alternative Dispute Resolution (ADR)

CENTRUM GLOBAL B V will ensure that it:

- must provide players **free access** to an **independent CGA-certified ADR provider**.
- must upload an agreement with at least one certified ADR entity to the CGA portal within one month of certification listing.
- must include ADR details in all complaint correspondence and in the organisations Terms and Conditions.

8.9 Authority Escalation

CENTRUM GLOBAL B V will ensure that it:

- must clarify it is **not the CGA's role** to mediate individual complaints.
- allow all Players to escalate matters of regulatory breach to the CGA via their **online form**.
- allows the CGA to use this information for **supervisory purposes**.

8.10 Contact Points for Complaints

CENTRUM GLOBAL B V must accept complaints via Email.

8.11 Record-Keeping

CENTRUM GLOBAL B V must log and securely store **all complaints for five years**, including:

- Resolved (upheld or rejected)
- Unresolved
- Escalated to ADR or legal proceedings

8.12 Regulatory Reporting

CENTRUM GLOBAL B V will ensure that a report will be submitted to the CGA **biannually on January 15th and June 15th**, detailing:

- Total complaints received
- Resolved and pending complaints
- Complaint categories
- ADR cases and outcomes
- Legal actions taken by players

8.13 Visibility in Terms and Conditions

CENTRUM GLOBAL B V must display the complaint procedure:

- As a **standalone document** or link.
- Within the **Terms and Conditions**.
Including:
 - » Player rights and complaint steps,
 - » Timeline expectations,
 - » ADR and CGA contact details,
 - » Legal implications of ADR decisions.

9 Alternative Dispute Resolution Policy

9.1 Alternative Dispute Resolution Policy Aim

CENTRUM GLOBAL B.V. must ensure players have access to a transparent, fair, and independent ADR process when complaints are unresolved through internal procedures.

9.2 Obligation to Offer ADR

CENTRUM GLOBAL B.V. must:

- Provide players with access to at least **one CGA-certified ADR provider**.
- Ensure that the ADR process is **free of charge** for players; all ADR-related costs are the responsibility of CENTRUM GLOBAL B.V.
- Include full ADR details (contact information, process, player rights) in the **Terms and Conditions** and all complaint-related communications.

9.3 Process Requirements

CENTRUM GLOBAL B.V. must:

- Notify the player of the right to escalate to ADR when a complaint remains unresolved.
- Share all relevant documentation and case details with the ADR provider upon request.
- Remain actively engaged and responsive throughout the ADR process, including fulfilling any reasonable information requests by the ADR entity.

9.4 Operator Non-Participation

CENTRUM GLOBAL B.V. must avoid conduct that obstructs ADR proceedings:

- Failure to participate or to supply necessary information may result in a default decision made in the player's favour.
- The ADR provider is required to notify the CGA within **one week** of CENTRUM GLOBAL B.V.'s non-cooperation, constituting a breach of licensing obligations.

9.5 Binding Nature of ADR Decisions

CENTRUM GLOBAL B.V. must:

- Treat all ADR decisions as **binding**, implementing them promptly and in full.
- Respect the player's right to **further legal or judicial recourse**, as ADR outcomes do not preclude court action.

9.6 Transparency and Disclosures

CENTRUM GLOBAL B.V. must clearly inform players about ADR availability and procedures:

- Identify the ADR provider and confirm CGA certification.
- Explain that ADR services are free for players.
- Advise players of their right to legal representation and to withdraw from the ADR process.
- Provide all necessary contact and procedural information in a manner that is easy to find and understand.

9.7 Recordkeeping and Communications

CENTRUM GLOBAL B.V. must:

- Maintain full records of all ADR referrals, communications, and outcomes.
- Respond promptly to ADR provider communications, supplying additional evidence or clarifications as required.
- Keep players informed throughout the ADR process, including updates on timing, delays, and final outcomes.

9.8 Reporting and Monitoring

CENTRUM GLOBAL B.V. must cooperate with the CGA in its monitoring role:

- Be prepared to provide access to all ADR-related records upon request.
- Take note of operator performance issues or systemic concerns raised in ADR quarterly reports and implement necessary corrective actions.

CENTRUM GLOBAL B.V. shall maintain statistical data regarding ADR cases as required by CGA and will submit quarterly or ad hoc reports upon request.

9.9 Continuity of ADR Service

If an ADR provider loses CGA certification, CENTRUM GLOBAL B.V. must:

- Cease referring new complaints to the uncertified provider immediately.
- Be informed of the decertification by the ADR provider within **two working days**.
- Arrange transfer of ongoing dispute cases to a certified ADR provider, or complete them with CGA approval, keeping affected players fully always informed.

10 Staff recruitment, education, training and development

10.1 Importance for AML/PTF/PFP risks

The way the company is organised can increase or mitigate the exposure of the company to money laundering and terrorist financing risks. In particular procedures and controls operated by the company, many of which are required by law, can be applied in order to manage AML/PTF/PFP risk.

10.2 The importance of staff in ML prevention

Success in preventing money laundering and terrorist financing cannot be achieved by having appropriate policies alone. Even the best policies are useless if staff ignore or circumvent them, whether through ignorance, carelessness or deliberately. Staff are a business's strongest defence or their weakest link. It is therefore essential that the principles outlined in section **Error! Reference source not found.** are adhered to.

10.3 Human Resources risk factors in ML prevention

The main human resources risk factors are:

- Staff lack integrity
- Staff lack knowledge, training or awareness
- Staff have conflicts of interest
- Direct criminal or terrorist exploitation of HR weaknesses.

10.4 Integrity

The integrity of the directors and employees of the company are the foundation of its AML/PTF/PFP measures. If staff lack integrity there is a danger that they may become involved in or become willing accomplices to laundering activity.

Direct involvement in laundering operations is the possible extreme. More likely is that staff without the right attitude are unlikely to:

- Maintain awareness and detect money laundering
- Report money laundering if they become aware of it
- Take seriously their own training or that of their subordinates
- Encourage reporting and foster a culture that supports money laundering prevention.

10.5 Staff Recruitment

It is important that we take appropriate steps to ensure the integrity of new staff. Such steps should be risk based, with the extent of the effort proportional to the role of the employee and the money laundering threat inherent in the role they are being recruited for.

The following staff screening procedures are operated by Centrum Global B V:

- For all new staff at least one reference will be taken up. References will be obtained by obtaining the permission of the prospective employee to write direct to the referee. References supplied by the prospective employee and references addressed "to whom it may concern" will not be accepted unless they can be confirmed direct with the referee.

For staff recruited for Manager, MLRO or Director positions, the following additional checks will be performed:

- The identity of the prospective employee will be verified by requesting sight of identity verification documents.
- NAMESCAN or Similar
- A police vetting form submitted to the CGA prior to appointment

10.6 Staff Knowledge, Training and Awareness

Recruiting staff of integrity is not sufficient in itself. Staff must have sufficient awareness and training to detect money laundering and terrorist financing and to understand what is expected of them.

It is key to effective AML/PTF/PFP arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.
- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering
- Staff are aware of their personal legal obligations

The steps adopted by the group to ensure staff have appropriate awareness and training are as follows:

- All new staff will receive AML/PTF/PFP induction training, to include:
 - » The provisions of the AML/PTF/PFP code and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
 - » Their personal obligations under the AML/PTF/PFP Code and associated personal liabilities for non-compliance
 - » The internal reporting procedures detailed in the AML/PTF/PFP Manual
- AML/PTF/PFP refresher training will be delivered at least annually for all staff.
- The MLRO will provide other ad hoc information about news and developments. This will be targeted as appropriate.
- The MLRO will send periodic reminders of the need to report certain matters.

10.7 Compliance with company policies and procedures

Failure to comply with Company policies and procedures may result in disciplinary action being taken against you which may include summary dismissal.

10.8 Technological Developments

Centrum Global B V recognises the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The whole company (inc Directors) retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the company has engaged with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- Centrum Global B V is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

11 Policy Review / Audit and Independent Testing

11.1 Policy Review and Audit

CENTRUM GLOBAL B.V. ensures that all core regulatory policies — including AML/PTF, Player Complaints, Responsible Gaming, and ADR are subject to periodic review. This includes:

- Annual review by the Compliance Officer or MLRO.
- Audit at least annually by either:
 - » An internal audit function independent from policy authorship; or
 - » A qualified third-party external auditor.

Audit reports and reviews shall be retained and made available to the Curaçao Gaming Authority upon request.

11.2 Independent Testing and Software Certification

CENTRUM GLOBAL B.V. acknowledges the CGA's Guidelines for the Certification of Independent Gaming Test Houses and supports the requirement for integrity and fairness in all software components used in wagering operations. Where applicable:

- All game mechanics or result-determining algorithms shall be subject to certification by an approved CGA test house.
- If CENTRUM GLOBAL B.V. develops or deploys proprietary software that impacts game or payout outcomes, it shall be submitted for independent certification before use.
- CENTRUM does not currently offer retail-facing RNG-based games but will comply with this requirement if future product lines require it.

12 Version Control

Name	Description
Document Name	AML Guide
Version	1.0_25
Author	Christian Heap
Authorised By	Dennis Verrios
Distribution Date	01/02/2023
Review Date	01/03/2023

13 Appendices

13.1 Appendix A – Suspicious Transaction Report

Report Prepared by:	
CLIENT Name	
CLIENT ID	
Address	
Email &/or Telephone	
Is identification and address verification held?	
Is enhanced due diligence held?	

Reason for suspicion	
To include: <i>Identification verification</i> <i>Criminal conduct known or suspected.</i>	

Date of report	
-----------------------	--

To be copied, and one copy completed below returned to the staff member as acknowledgement. Remember you are required to do nothing that might prejudice inquiries i.e. tipping off the client or any other third party.

Receipt of report acknowledged:	
Signed MLRO	
Date	