

GARETON B.V.

V 1.1

Document

**Anti-Money Laundering/Combating
Financing of Terrorism and Financing of
Proliferation of weapon and mass
destruction (AML/CFT/CFP) Manual**

Content

INTRODUCTION	3
PROCEDURES	4
KEY RESPONSIBILITIES	4
PROVISION OF EDUCATION AND TRAINING	5
RISK ASSESSMENT	5
A POLITICALLY EXPOSED PERSON	6
SANCTIONS	7
DEALING WITH SANCTIONED PERSONS	7
LOCATION OF PARTNER	8
AMOUNT OF FUNDS BEING TRANSACTED	8
NATURE AND FREQUENCY OF TRANSACTIONS	9
SOURCE OF FUNDS BEING TRANSACTED	9
PLAYER RISK MATRIX	10
Managing Risks Related to Crypto Transactions	11
POLICY AND PROCEDURES	11
IDENTIFICATION	11
ANONYMOUS ACCOUNTS	12
EVIDENCE OF IDENTITY FOR PARTICIPANTS	12
ENHANCED DUE DILIGENCE	14
SOURCE OF FUNDS AND WEALTH	15
KYC MATRIX	16
ONGOING MONITORING	17
ONGOING MONITORING OF TRANSACTIONS	17
ONGOING MONITORING OF CUSTOMER DATA	17
RECORD KEEPING AND RETRIEVAL OF RECORDS	18
RECORD OF TRANSACTIONS	18
RETENTION OF RECORDS	19
MLRO AND MLCO	20
REGISTER OF MONEY LAUNDERING ENQUIRIES AND REPORTS	20
INTERNAL PROCEDURES INCLUDING THE REPORTING OF SUSPICIOUS TRANSACTIONS, BOTH INTERNAL AND EXTERNAL	20
INTERNAL SUSPICIOUS ACTIVITY REPORTING	20
REPORTING AND 'ACTIVE' BUSINESS	21
EXTERNAL SUSPICIOUS ACTIVITY REPORTING	21
WHISTLEBLOWING POLICY	22
STAFF EDUCATION, TRAINING, AND DEVELOPMENT	22
IMPORTANCE FOR AML/CFT/CFP RISKS	22
THE IMPORTANCE OF STAFF IN ML PREVENTION	22
HUMAN RESOURCES RISK FACTORS IN ML PREVENTION	22
INTEGRITY	23
STAFF RECRUITMENT	23
STAFF KNOWLEDGE, TRAINING AND AWARENESS	23
STAFF PROMOTION AND TRANSFER	24
TECHNOLOGICAL DEVELOPMENTS	24
PROCEEDINGS	24
	1

OFFENCES	24
VERSION CONTROL	25
APPENDICES	26
APPENDIX A SUSPICIOUS ACTIVITY REPORT	26
APPENDIX B BANNED COUNTRIES	28

Introduction

The aim of this manual is to set out the policies, procedures, systems and controls necessary to meet the obligations of the Company that operates from Curacao and is held to compliance with National Ordinance on identification when rendering services (NOIS) and National Ordinance on the reporting of unusual transactions (NORUT) and the Sanction National Ordinance and the Kingdom Sanction Act.

With the publication of the National Decree supervisor identification when rendering services gaming sector and the National Decree supervisor unusual transactions gaming, the Curaçao Gaming Control Board (GCB) is tasked with the Anti-Money Laundering, Combating of Terrorist Financing & Combating of Financing of Proliferation (hereinafter referred to as: AML/CFT/CFP) supervision of the gaming sector operating in and from Curaçao.

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 a process of making dirty money looks clean.

Please note that there are many predicate offences for money laundering such as human trafficking, arms trafficking, fraud, corruption, kidnapping and tax crimes.

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 terrorist 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 funds, FT is mostly concerned with obscuring the end recipient of the funds.

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.

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

- Identification
- Record keeping

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

It is the Company's policy that NOIS and NORUT 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 minimize 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 Government of Curacao legislation.

The Company 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 Curacao Financial Intelligence Unit (FIU) and thereafter shall be undertaken in conjunction with the relevant Government of Curacao authorities and in accordance with Curacao custom and practice to avoid any risk of the Company committing a tipping-off offence.

The Company's policies and procedures are based upon the regulations referred to above and associated guidance issued by the Curaçao Gaming Control Board.

Procedures

- 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 business partners 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).
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation.
- All suspicions are reported promptly to the MLRO.
- That the Company's vigilance systems are implemented and regularly monitored.

Key responsibilities

The Company's management is responsible for:

- The day-to-day compliance with AML/CFT/CFP obligations within the areas of the Company for which they are responsible.
- Ensuring that the MLRO is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the MLRO and AML/CFT/CFP Compliance Officer with the appropriate resources to fulfil their functions effectively.
- Ensuring that the MLRO 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.

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 the FIU.
- All contact between the Company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.
- Establishing the suspicious reporting process and ensuring that this process is understood by all staff.
- Maintenance of the register of internal and external disclosures and register of money laundering and financing of terrorism enquiries.

AML/CFT/CFP Compliance Officer is responsible for:

- Establishing, recording, maintaining and operating appropriate procedures and controls for monitoring and testing compliance with the AML/CFT/CFP legislation.
- Adopt policies which manage the risks identified by the Company's business risk assessment, monitor the performance of these policies and address any deficiencies identified.
- Submission of a report, on at least an annual basis, to the Company's senior management that describes:
 - Any new developments within the industry in relation to AML/CFT/CFP including updates to any legislation or regulatory guidance.
 - Any updates to the Company's internal AML/CFT/CFP procedures and policies.
 - Any activities relating to compliance with the NOIS and NORUT.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the MLRO 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.

Provision of Education and Training

All members of management and staff will receive initial training and on-going training at least on an annual basis or as and when required.

Risk Assessment

As part of the companies regulated approach to AML/CFT/CFP risk the following assessment has been conducted 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.

A Politically Exposed Person

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption. Therefore, full enhanced due diligence must be conducted upon any identified PEPs. The Company does not distinguish between foreign and domestic PEPs, all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

Screening is undertaken by the Company with the help of automated tools as well as using the third party KYC6 service provided by Acuris Intelligence to identify PEP and Sanctioned individuals upon customer registration/deposit. This will also pick up on any adverse media relating to the customer.

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- 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 organization.

A PEP also includes family members and close associates of the above, including:

- A spouse;
- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;
- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;
- A person in a position to conduct substantial financial transactions on behalf of a PEP.

Gareton B.V. has made the decision to not accept PEPs as customers, as they fall outside the Company's risk appetite.

Sanctions

Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals where diplomatic efforts have failed. Sanctions can take form of economic, trade, financial services, or international movement (travel bans) prohibitions.

UN Sanctions

The United Nations Security Council publishes the names of individuals and organizations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN has in place other sanction lists pertaining to other jurisdictions, entities, and individuals, including wider terrorist activity under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regimes: <https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about the UN sanctions regimes.

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them.

The OF AC Sanctions List Search is available at the following link:

<https://sanctionsscarch.ofac.trcas.gov/>

Dealing with sanctioned persons

In case when the Employee during Client on-boarding, COD or EDD procedure, or during Client ongoing monitoring becomes in the possession of the information that the Client is a sanctioned individual or has any links to sanctioned individuals and/or entities, he MUST:

- Immediately freeze all the funds / economic resources of the Client available to the Company;

- Not enter into any financial transactions or provide financial assistance or services to the Client;
- Apply Enhanced Due Diligence measures;
- Immediately inform and file the internal report to the MLRO;
- Suspend the account of the Client until further instructions from the MLRO.

It is prohibited to inform the Client or any third party (except a senior manager or MLRO) in advance, that a freezing measure is to be applied.

The MLRO has to review the internal report as soon as practicable and, in case there are reasonable grounds to suspect that the Client is the sanctioned individual from the lists provided by OFAC, EU, UN or national Sanctions regimes, the MLRO will cease to conduct any further business and a report will be submitted to the FIU.

Location of Partner

A customer located in a jurisdiction which is not Financial Action Task Force ("FATF") compliant (named on FATF's List Black or Grey), may generally be considered to represent a potential risk of money laundering or terrorist financing activity. However, whilst the Company considers a customer located in a jurisdiction named on List A to be of high risk, it is management's considered opinion that an individual transacting with the Company in what may be considered a normal manner, but from a jurisdiction listed on Grey List, represents only a minimal risk of money laundering or terrorist financing.

Therefore, customers located in jurisdictions named within the Black List will be automatically subjected to enhanced due diligence and subject to a higher degree of monitoring. However, with regards to partners resident in jurisdictions that are named within the Grey List, management considers that only with other factors, when combined with the above, create heightened risk of 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
- Source of funds being transacted and the destination of the withdrawals
- Source of wealth
- The location from where the customer is accessing the platform from, if different to the registered jurisdiction (detected via IP or device checks).

A quarterly review is conducted across all registered participant jurisdictions. The review encompasses both AML/CFT/CFP and commercial considerations. The quarterly overview of the jurisdictions takes place in order to check that players have not been accepted from FATF closed or deficient jurisdictions. This review is monitored and reviewed by the senior management including the MLRO.

Amount of funds being transacted

If funds deposited or withdrawn by a Customer are over EUR 2,000 (or currency equivalent) or aggregate in excess of EUR 2,000 (or currency equivalent) in any thirty day period (qualifying payment), there is an enhanced risk of money laundering or terrorist financing activities and identity verification checks are undertaken. Such customers will be deemed as a medium risk.

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.

If funds deposited or withdrawn exceed 10,000 EUR (or currency equivalent) or aggregate in excess of EUR 10,000 (or currency equivalent) in any period (enhanced qualifying payment), there is an even further enhanced risk of money laundering and terrorist financing. Therefore, any customer that reaches these thresholds will automatically be deemed high risk and subjected to enhanced due diligence measures.

When a customer reaches either the threshold for medium or high risk measures, the transaction that they are attempting (either a deposit or withdrawal) will not be permitted until they have satisfied their standard or enhanced due diligence requirements accordingly.

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, unless they reach the thresholds. Irregular patterns of activity or regular deposits and withdrawals with limited betting transactions may highlight enhanced risk both from an AML/CFT/CFP and social responsibility perspective. Participants managing their payments and withdrawals to remain non-qualifying may also represent enhanced potential 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.

Several changes to a customer's transactions may prompt an investigation, requiring the customer's identity to be verified and potentially for the customer's source of wealth to be established. Source of wealth checks will establish both the legitimacy of the customer's funds and as to whether they can afford their current levels of spending. Such checks will be conducted on a case-by-case basis.

Multiple accounts are not permitted on the platform. This risk is mitigated by the system automatically preventing registration with matching emails, usernames, first names and surnames. However, there is always the possibility that an individual has used false registration details or details that are not theirs to create several accounts. Multiple accounts can be used to carry out multiple smaller transactions in an attempt to avoid triggering any due diligence thresholds. Ongoing monitoring practices will be utilized to analyze transactional patterns, similar registration details, matching IP and device data in order to detect multiple account abuse. In such circumstances these individuals will be automatically banned from the platform unless a reasonable excuse can be provided from the customer.

Source of funds being transacted

The source of the funds will be verified to be coming from a legitimate source with legitimate connections to the customer. Any contradictions to this will result in the customer's account being suspended either indefinitely or until a reasonable explanation be provided.

All withdrawals should be sent to the source from which the customer deposited. However, should the customer have a legitimate reason as to why this is not possible (e.g. the closure of a bank account), relevant documentation must be submitted by the player demonstrating the reason why

the payment source is now not available and that the customer is the owner of the new payment method.

Multiple changes to the source of funds when multiple transactions are being made should also be queried by the Company as this is a potential indicator of money laundering. Should the customer make a change of their source of funds 3 times, then they will be deemed medium risk and subjected to due diligence checks. Should the customer make a change of their source of funds 5 or more times, then they will be deemed high risk and subjected to enhanced due diligence checks.

Player Risk Matrix

Risk rating	Nature	Location	Source of funds/ Wealth	Transaction size
Prohibited	Sanctioned individual or entity A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements Anyone deemed to be linked with the financing of terrorism Business participant	Closed jurisdictions A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/ EDD requirements	Cash A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements Funds appear to be generated or linked to the proceeds of crime	A customer that has breached any of the below thresholds but does not comply with the Company's CDD/ EDD requirements
High	PEP Any individual or entities subject to warnings Professional gambler Customers that are sporting professionals betting on sports High net worth individuals	Named on FATF's Black List . Countries with AML/CFT/CFP strategic difficulties	Use of over 5 different payment methods	Deposit or withdrawal of EUR 10,000 in any period

Medium	Public profile raises some form of concern e.g. adverse media, social media activity	Named on FATF's List B. Countries which in the opinion of the MLRO represents heightened risk	Use of voucher or pre-paid card Where the method of withdrawal differs to that of original deposit Use of over 3 different payment methods	Deposit or withdrawal of over EUR 2,000 (or currency equivalent) or aggregate in excess of EUR 2,000 (or currency equivalent) in any 30-day period
Low	Individual	Fully compliant with FATF No AML/CFT/CFP concerns	Bank transfer Debit or credit card Approved payment service provider	Under any of the qualifying payment thresholds

Following the risk assessment, customers will be identified as either low, medium, high or will not be able to open an account. 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.

The Company will undertake a review of the relevance of its risk assessment as part of the AML/CFT/CFP Compliance Officer's annual report to senior management or as and when significant changes in business operations dictate.

Managing Risks Related to Crypto Transactions

Due to the unique risks associated with cryptocurrency transactions and have developed specific strategies to address these challenges. We take a proactive approach to ensure the security and legitimacy of crypto-related activities on our platform. Recognizing the volatility and potential risks of cryptocurrencies, we employ a risk-based approach that allows us to set transaction limits, define acceptable currencies, and customize risk thresholds based on our risk tolerance levels.

In order to minimize exposure to illicit activities, we screen crypto wallets against publicly available databases of known high-risk or blacklisted addresses associated with criminal activities, fraud, or sanctioned entities. This helps prevent transactions from being processed to or from wallets flagged for illicit activity.

Policy and Procedures

Identification

The Company does not allow online gaming or the depositing of funds for the purpose of online gaming unless the intended participant has:

- Registered with the company through the registration page at the respective domain operated under the gaming license and
- created an account with the company and
- confirmed their acceptance of the terms and conditions.

To register, a customer must provide the company with details of their:

- First Name
- Last name
- Username (chosen)
- Date of Birth
- Email Address
- Residential Address
- Nationality

Participants registering on the site are required to input a password of their choosing. No player under the age of 18 can register with the company. If their age is below 18, they are unable to register.

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

Records will be maintained by the Company's administration of all current, attempted and past registrations.

Upon completion of all required fields 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 fields are not completed. To activate the player will be required to re-log on to the respective domain using the link provided, upon successful input of their password their account will be activated.

No monies can be deposited with the company and no bonuses allocated to the account until the account has been activated.

Anonymous Accounts

Customers will not be able to register with fictitious names or anonymous accounts.

When registering with a website owned by the Company, the account will not be opened unless the requested identity details (shown above) are completed in full. Duplicate accounts will not be allowed, and checks will be made at the time of registration.

Fictitious names will not be allowed. Obvious fictitious names will be identified at the time funds are deposited to the account and the account will be terminated.

A participant whose account is terminated will be advised by email unless it is in relation to a matter reported to the FIU, in which circumstances please be advised accordingly by the MLRO.

Evidence of identity for participants

Payments made to participants that exceed EUR 2,000 (or currency equivalent) or payments which taken cumulatively within a 30 day period exceed EUR 2,000 (or currency equivalent) are classified as qualifying payments and as such trigger the requirement for evidence to be gathered confirming the registered participant's identity.

When a participant requests a qualifying payment from the company or when a participant wins an amount which will be deemed a qualifying payment, the payment will be stopped, and the account immediately suspended from betting activity.

Similarly, should a customer be deemed medium or high risk for another reason, the customer will also be subject to the following requirements.

An email will be sent automatically to the participant explaining why the payment has not yet been made and the account's activity suspended, and the following verification procedure will take place

a) Verification of identity:

The verification of identity may be completed via the verification screening conducted upon registration/first deposit depending on the information gathered. Should the screening report support enough information whereby the customer's name, address and date of birth can be relied on as being accurate then that will be sufficient for this purpose and no further information will be required from the customer. However, consideration must also be applied should there be any other suspicion, for example if you suspect that the customer is underage and is using the details of an adult to register on the platform. In such circumstances further due diligence items should be requested from the customer.

As part of the screening report, PEP, sanction and adverse media checks will also be made.

When requesting due diligence from the customer to verify their identity, the following are acceptable identity documents:

- A passport
- A national ID card
- An armed forces ID card
- A full driving license

To be acceptable identity documents must be:

- A good clear high-quality color scanned copy, plainly legible,
- Unexpired at the date of receipt,
- Bear a photo of the holder, and
- Signed by the holder

b) Verification of address:

- A recent account statement (i.e. no more than 6 months old) from a recognized bank, building society or credit card company or the most recent mortgage statement from a recognized lender.
- An unexpired photographic driving license 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 6 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 Known lawyer's confirmation of property purchase or legal document recognizing the title to the property.
- Documents provided to verify an address should not refer to P.O. Boxes or care of addresses.
- Physical verification of address made by sending letter requiring action from the customer to confirm receipt.

For all documents, the documents should be reviewed to check the following:

- That they appear valid (e.g. the correct layout, format and style)
- That they do not appear to have been tampered with, have not expired and are within the permitted timeframes (i.e. not over 6 months for bill and account statements)
- The algorithm/MRZ on passports.

The email requesting due diligence from the customer will automatically be copied to the Administration Team. The Administration Team will log the email and await receipt of the required documents.

Should there be doubts as to the validity of a document or whether it genuinely belongs to the customer, consideration should be made as to whether the documents should be certified or that a 'selfie' photograph or video of the customer holding the document be submitted.

The account will be deemed medium risk. Only upon receipt of the documents to a satisfactory standard will management authorize the re-activation of the account and process the qualifying payment.

The account will be marked as having passed basic customer due diligence, and the account's risk level may then be deescalated to low risk should no other concerns be present. A log must be kept recording the change in risk levels and the rationale for the change.

Open-source checks should also be conducted should there be any adverse media on the customer not detected by the verification screening checks, or to pick up on any social media that may raise further suspicions. Examples to look out for include:

- they appear to be resident in a jurisdiction different to that provided upon registration
- their lifestyle is not reflective of their level of spending on the platform
- they appear to be under the age of 18 or of a different age that to that provided upon registration
- they appear to be linked to criminal activity or terrorist organizations

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

- If the required documents are not received and the monies and account remain suspended after 4 weeks.
- 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
- Multiple use of payment methods
- 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
- Any suspicions arise from conducting open-source checks

If suspicious activity is considered a possibility a suspicious transaction report will be lodged.

Enhanced Due Diligence

In certain cases, highlighted by the risk assessment, the Company 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 recorded as high risk within the administrative system and a report of their transactions and any other relevant information made available to the MLRO.

Enhanced due diligence will consist of the requirements as established for standard customer due diligence, in addition to the following:

- Requirement of additional identification data (middle names, former names, aliases, occupation, employer, personal identification number, previous addresses)
- Consideration as to whether this data needs to be further verified (additional identity documents, telephone or video call with the customer, 'selfie' with the identity document, certified documents)
- Establish the source of funds
- Establish the source of wealth
- Flag the participant for enhanced on-going monitoring
- Consideration of a further 3rd party background check
- Open source checks

A customer that is deemed high risk and has complied with all EDD requirements will be referred to a senior manager or the MLRO for approval before the customer is permitted to continue with any further activity on the platform.

When either standard due diligence or EDD has been requested from the customer, all deposits and withdrawals will be suspended until the items have been provided and the Company is satisfied that the customer has no connection to money laundering or terrorist financing. Following the request, the customer will have a period of 7 days during which they may continue to bet using the balance already held on the platform, after which all activity will be suspended until due diligence requirements have been satisfied. If it is believed that due diligence has not been complied with due to suspicious reasons, then this should be reported to the MLRO.

A participant who poses a higher risk may be:

- a PEP
- Resident in a country which the company has reason to believe does not apply or insufficiently applies the FATF recommendations.
- Professional gambler
- Sporting professionals betting on sports
- Meets the EDD requirement on the risk matrix due to their level of transactions
- Meets the EDD requirement on the risk matrix due to the number of changes to their payment method.
- Any persons who are the subject of any warnings or notices.
- A combination of medium risk factors, such as reaching a qualifying payment threshold whilst being resident in a medium risk jurisdiction. To be judged on a case-by-case basis.

Source of Funds and Wealth

Source of funds is quite simply the method by which the customer has deposited funds onto the platform. This should be easily identified upon the customer depositing, as the system should detect the method being used e.g. debit card or payment wallet.

Should the system not recognize the payment method, is a method unauthorized to be used on the platform, or the payment details do not match with that of the registration, all activity on the account will be suspended and the matter reported to a senior manager or MLRO.

Source of wealth is how a person has generated the money they are spending on the platform and their financial standing in general. When conducting enhanced due diligence, reasonable measures must be made to establish source of wealth.

Source of wealth can often be satisfied by finding information in the public domain. An open-source check can offer insight into an individual's lifestyle, their occupation, the area they live and type of home that they occupy. This information can often be found on a customer's social media account and/or looking up their address using Google Maps. Any adverse media or and media coverage in general may be picked up using verification screening systems and open-source checks respectively.

Where verification screening and open-source checks do not provide satisfactory results, documents may be requested from the customer to demonstrate their source of wealth, for example a pay slip or a contract of employment. Open-source checks can often shed light upon an individual's current employer. Each customer's source of wealth may differ entirely and therefore different approaches may need to be undertaken depending on the circumstances.

When reviewing the source of wealth information, the Company staff will need to consider how reliable or independent the source of the information is, how plausible the information is, and how this compares to the customer's activity.

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:

Due diligence check	Low	Medium	High
PEP, Sanction and adverse media Screening	x	x	x
Identity Verification Screening	x	x	x
Request ID and address documents		x	x
Open source checks		x	x
Source of funds	x	x	x
Source of Wealth			x
Additional identity and address documents			x
Additional 3rd party verification screening			x

Ongoing Monitoring

All transactions by all customers are recorded and can be reported on an ad-hoc basis for monitoring purposes. It is recognized that a significant change to the normal operation of an account could be a sign of suspicious activity. A change may be:

- Unusually large transactions based on past deposit account history.
- Multiple changes to address details.

In addition, changes made to the partners identity and personal information will be reported on to the Company's management and recorded appropriately. The evidence of identity previously provided by the partner will be reviewed and steps taken to renew and update that information reflecting the reported changes to the partner's identity. In certain cases, this may mean any business is suspended pending receipt of new identity and address verification.

In the event that satisfactory confirmation of the information as to the identity of the partner or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further trading allowed, and consideration be given to the lodging of a suspicious transaction report.

Ongoing Monitoring of Transactions

All transactions by all customers are recorded and can be reported on a daily, weekly, monthly, or annual basis.

It is recognized that a significant change to the normal operation of an account could be a sign of suspicious activity. A change may be:

- Unusually large deposits based on past deposit history
- Unusual patterns in betting activity
- Large deposits followed by large withdrawals combined with minimal betting transactions
- Multiple changes to deposit and withdrawal methods

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 due diligence 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.

Transaction reports will be reviewed on a monthly basis, overseen by the MLRO. Particular scrutiny will be applied to medium and high-risk customers. Where the activity is deemed to be unusual, an investigation into the customer may begin which may include asking the customer for their rationale for carrying out the activity or further information or evidence of the source of funds or source of wealth.

Ongoing Monitoring of Customer Data

Changes made to a customer's identity and personal information will be reported on to the Company management. The evidence of identity previously provided by the participant will be reviewed and steps taken to renew and update that information considering the reported changes to the

participants identity. In certain cases, this may mean that the account is suspended pending receipt of new identity and address verification.

Of course, there are many acceptable reasons as to why a person's identity information may change, for example getting married and changing their surname to that of their spouse. However, differing identity details may be due to having previously provided false details due to an attempt at some form of criminality.

In such circumstances, the verification procedures shall be followed in addition as to the customer providing reasoning for the change in details.

Should a customer's risk level increase (e.g. from low risk to medium risk) and due diligence documents are already held on the customer, consideration must be made whether further documents must be submitted. The previously supplied documents must be reviewed to ensure that they are not expired, in such circumstances up to date documents must be requested.

CDD/EDD held will be reviewed on an annual basis regardless of any changes to the customer's circumstances.

In the event that satisfactory confirmation of the information as to the identity of the participant or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further betting activity allowed, and consideration be given to the lodging of a suspicious transaction report.

Record keeping and retrieval of records

Record of Transactions

The Company will maintain appropriate records of all participants and their associated transactions. The MLRO has 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 identity

The MLRO will at all times 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 has the ability to retrieve all identity verification that has been collated on all customers. This includes all correspondence between the Company and the customer, plus any notes and internal investigations conducted on customer activity.

- Deposits, withdrawals, bets, prize payments, credits

All financial transactions are recorded against the customer within the back-office system and are reconciled against source of funds data. 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 (credit/debit card, e-wallet etc.)

All financial transactions are maintained in a system audit log which is available to the MLRO at all times.

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 scrutinized by the MLRO by date, participant or nature of the transaction.

- Internal compliance documents – policies and procedures, internal and external registers and reports, risk assessments, staff vetting and training, reports prepared by the AML/CFT/CFP Compliance Officer for the management.

All internal compliance documents will be held on the back-office system, with the MLRO having full access.

Retention of Records

All the above-named records will be maintained in a secure and accessible form. Secure backups are made daily of the following customer data:

- Records
 - all registration details
 - identification verification details
 - standard and enhanced due diligence items
 - suspended accounts and reason for suspension
 - closed accounts
 - financial transactions – deposits, bets made, withdrawals, prize payments
 - self-exclusion periods (temporary and permanent)
 - self-imposed limits
 - excluded players
 - complaints and responses
 - audit trails
 - bank reconciliations
 - Customer Service electronic correspondence records

Records associated with a customer (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the customer's account or the date of the last transaction.

Records associated with the register of internal and external disclosures and the register of money laundering and financing of terrorism enquiries will be maintained for a period of 5 years following the finalization of the relationship with the related parties or for the period as advised by the FIU.

MLRO and MLCO

Register of Money Laundering enquiries and reports

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

- a) Enquiries made to the Company 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)

- b) All reports made to a representative within the FIU in relation to suspicious transactions.

This register contains:

- The name of whom the report is made (MLRO)
- Relevant dates of the suspicious activity and when internal and external
- Information about the activity which is sufficient to identify the grounds for suspicion
- The reference number supplied by the FIU
- Outcome of enquiry (if known)
- Any other disclosure made to the FIU for intelligence purposes only

- c) All reports made to the MLRO by the Company 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
- Whether or not it was escalated to be reported to the FIU
- Outcome of the report

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

The Company shall at all times have an appointed MLRO. 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 will have unfettered access to all reports, transaction histories, complaints and audit trails.

Internal suspicious activity reporting

Suspensions must be reported to the MLRO as soon as reasonably practical using the attached form, as per Appendix A. The form is also available on request from the MLRO. The case may be discussed

initially with the MLRO, 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. It is necessary for the person making the report to include their name on it. 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.

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. 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.

The MLRO in conjunction with the Directors will manage the process of ensuring that the transaction may proceed, including obtaining FIU clearance if appropriate.

External suspicious activity reporting

The MLRO 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 considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO is responsible for:

- Submitting the necessary information to the FIU.
- Recording the disclosure in the register of disclosures.
- Dealing with subsequent production or account monitoring orders if there are any.

Tipping Off/Confidentiality

Any person must treat any information where that person knows or suspects that an unusual transaction report has been made or that an investigation is under way or proposed or strictly confidential.

No staff member may disclose to any person s/he has formed a suspicion that a person may be involved in suspicion that a person may be involved in suspicious matters or transactions or that a report has been lodged about that person with the FIU or any other authority.

Clear lines of reporting where matter or transactions are referred to the MLRO need to be maintained. All matters or transactions are to remain confidential between the reporting staff member and the MLRO.

It is an offense to disclose that an unusual transaction report or related information on a specific transaction has been reported to the FIU or that an investigation into money laundering, terrorist

financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

Whistleblowing Policy

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 the Company disclosure procedure set out in the Whistleblowing Policy:

- 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 they are 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.

Staff education, training, and development

Importance for AML/CFT/CFR risks

The way the company is organized can increase or mitigate the exposure of the company to money laundering and terrorist financing risks. Procedures and controls operated by the company, many of which are required by law, can be applied in order to manage AML/CFT/CFR risk.

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 defense or their weakest link.

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.

Integrity

The integrity of the directors and employees of the Company are the foundation of its AML/CFT/CFP 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.

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 the Company:

- 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 directly with the referee.
- Copies of relevant qualifications will be confirmed by requesting sight of certificates, copies of which will be retained on the employees file.
- Curriculum Vitae (CV) will be obtained from all prospective employees. The employment history included on the CV will be tested by taking a reference from a previous employer. This should usually be the most recent employer.
- Request details of any regulatory action or criminal convictions taken against the individual (or the absence of such action) and verify where possible.

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
- Third Party KYC service screening providers
- A police force vetting form

Staff Knowledge, Training and Awareness

Recruiting staff of integrity is not sufficient in of 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/CFT/CFP 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/CFT/CFP induction training, to include:
 - The provisions of the AML/CFT/CFP code and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
 - Their personal obligations under the AML/CFT/CFP Code and associated personal liabilities for non-compliance.
 - The internal reporting procedures detailed in the AML/CFT/CFP Manual.
- AML/CFT/CFP refresher training will be delivered at least annually for all staff and key persons.
- 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.

Staff promotion and transfer

When an employee is promoted or transferred to a new role the MLRO will be informed in advance, either electronically or in writing. The MLRO will confirm whether any further training or vetting is required, and whether the training or vetting is required before the appointment can take place.

Technological Developments

The Company recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The 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.
- The Company 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.

Proceedings

Offences

Any person who contravenes the NOIS / NORUT rules in regard to the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT/CFP) will be reported to The Financial Intelligence Unit of Curaçao.

In determining whether a person has complied with any of the requirements of any part of NOIS / NORUT a court may take account of any relevant supervisory or regulatory guidance which applies to that person and which is given by the Gaming Control Board.

Version Control

Document Name	AML/CFT/CFP Manual
Version	1.1
Author	Lydia Obispo
Updated By	N/A
Authorised By	
Distribution Date	17.04.2025

Appendices

Appendix A | Suspicious Activity Report

Report prepared by:	
Business partners	
Name	
Account ID	
Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	

Reason for suspicion	
To include: Identification verification Criminal conduct known or suspected	
Date of report	

Receipt of report acknowledged	
Signed MLRO	
Date	

Approval / Rejections				
Director	Signed	 Nathaniela Kwidama, Managing director o.b.o Allyant Group B.V.	Date	May 07, 2025
MLRO	Signed	 Lydia Obispo, MLRO o.b.o Allyant Group B.V.	Date	May 07, 2025
Development Review				
Responsible Person Review of Development	Date			
	<i>Review to comment on whether the development has been implemented in accordance with the outlined previously on this Form and whether a further risk assessment should be conducted</i>			
Approved	Director 1 Signed	 Nathaniela Kwidama, Managing director o.b.o Allyant Group B.V.	Date	May 07, 2025
	Director 2 Signed		Date	

Appendix B | Banned Countries

- Afghanistan;
- American Samoa
- Barbados
- Belarus
- Botswana
- Burundi
- Cambodia
- Central African Republic
- Cuba
- Ethiopia
- North Korea (DPRK)
- Democratic Republic of the Congo
- Fiji
- Guam
- Iran
- Iraq
- Lebanon
- Libya
- Lithuania
- Mali
- Mozambique
- Myanmar (Burma)
- Nicaragua
- Pakistan
- Palau
- Palestine
- Russia
- Samoa
- Senegal
- Slovakia
- Somalia
- South Sudan
- Sudan
- Syria
- Trinidad and Tobago
- Uganda
- Venezuela
- Yemen
- Zimbabwe
- Contested territories that are not internationally recognized:
- Eastern Ukraine, Transdniestria, The Crimea Region (Ukraine), Abkhazia, South Ossetia etc.

Title	AML policy Gareton B.V. new
File name	AML_policy_Gareton_B.V._new.docx.pdf
Document ID	6de9f2d068c687b403ca1a204cc770c820838c86
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History



05 / 07 / 2025
18:58:32 UTC

Sent for signature to lydia obispo
(lydia.obispo@allyant-group.com) from
timothy.becker@allyant-group.com
IP: 190.13.122.21



05 / 07 / 2025
19:28:24 UTC

Viewed by lydia obispo (lydia.obispo@allyant-group.com)
IP: 190.13.122.21



05 / 07 / 2025
19:29:08 UTC

Signed by lydia obispo (lydia.obispo@allyant-group.com)
IP: 190.13.122.21



05 / 07 / 2025
19:29:08 UTC

The document has been completed.