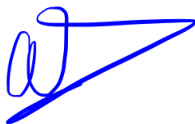


POLICY
For Prevention and Combating of Money Laundering Terrorist
Financing and Financing of Proliferation
GLADIA N.V



Version	Version Date	Approved By
		eMagnus Curacao B.V. Managing Director
3.0	13.05.2025	The Board 

ABBREVIATIONS

AMLTF&FP - Anti-Money Laundering Terrorist Financing and Proliferation Financing

ML - Money Laundering

TF - Terrorist Financing

FP - Proliferation Financing

WMD - Weapons of Mass Destruction

FATF - Financial Action Task Force

KYC - Know Your Customer

PEP - Politically Exposed Person

STR - Suspicious Transaction Report

MLRO - Money Laundering Reporting Officer

CO - Compliance Officer

CFO - Chief Financial Officer

KYC – Know Your Client

EDD - Enhanced Due Diligence

UBO - Ultimate Beneficial Ownership

PEP - Politically Exposed Person

This Policy aims to comply with the rules and guidance's contained in the following laws and Regulations:

- NATIONAL ORDINANCE of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance)
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (Regulations) effective as of January 9. 2025
- The National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92;
- 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).
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2)
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).
- Caribbean Financial Action Taskforce
- FATF recommendations

1. PREAMBLE

THE POLICY

The Policy on Prevention of Money Laundering and Terrorist Financing (hereinafter — «the Policy») outlines the general unified standards and procedures of anti-money laundering and combating terrorism financing which must be adhered to by GLADIA N.V (hereinafter — «the Company») its directors, officers and employees.

In any country or jurisdiction where the applicable anti-money laundering and terrorist financing laws and regulations require the Company to establish higher standards, such country standards must be adhered to.

Compliance with this Policy is mandatory and essential for ensuring that the Company is fully comply with applicable anti-money laundering and terrorism financing laws and regulations of respective countries and jurisdictions.

GLADIA N.V is committed to annual review and critical reassessment of this Policy in light of the company's business strategies, goals and objectives on an ongoing basis.

Definition of Money Laundering, Terrorist Financing, and Financing of Proliferation

Money Laundering - Money laundering refers to the process of concealing or disguising the true origin of proceeds derived from criminal activity, making them appear as though they come from legitimate sources or constitute legitimate assets. This process generally occurs in three stages:

Placement – At this stage, illicit funds are introduced into the financial system. This may involve converting the criminal proceeds into monetary instruments, such as money orders or traveler's checks, or depositing them into financial accounts.

Layering – In this stage, the funds are moved between various accounts or financial institutions to obscure their criminal origin and further distance them from the original illegal activity.

Integration – At the final stage, the funds are reintroduced into the economy, often used to purchase legitimate assets or to finance legitimate businesses or further criminal endeavors.

The goal of international anti-money laundering (AML) frameworks is to compel firms to:

Identify customers and detect suspicious transactions during the placement and layering stages.

Maintain adequate records to prevent the integration stage.

Provide an audit trail to assist investigators.

Report suspicious activities to the appropriate regulatory or legislative authorities.

Terrorist Financing

Terrorist financing involves the provision of funds to support terrorist activities, and it may not always be connected to proceeds from criminal conduct. Instead, it often involves concealing the origin or intended use of funds, which may come from legitimate sources such as charitable donations, foreign government support, business ownership, or personal employment.

While the motivation for financing terrorism differs from that of traditional money laundering, the methods of funding terrorist operations can often be similar to those used by criminals to launder money. Notably, funding for terrorism does not always require large sums of money; it can be accumulated over time and through relatively simple, low-value transactions that may not be complex in nature.

Financing of Proliferation

Financing of proliferation (FP) refers to the provision of funds for activities related to the development, acquisition, possession, or use of weapons of mass destruction (WMD) – including nuclear, chemical, or biological weapons – as well as their delivery systems and related materials. This includes actions such as manufacturing, transport, export, trans-shipment, brokering, stockpiling, or transferring these materials.

The Financial Action Task Force (FATF) defines proliferation of WMD as the transfer and export of nuclear, chemical, or biological weapons, their delivery systems, and related materials. While the issue of proliferation has been a focus of international attention for years, particularly with regard to nuclear materials (such as in the Nuclear Non-Proliferation Treaty), these conventions did not initially address the aspect of financing proliferation.

In 2004, the UN Security Council adopted Resolution 1540, which called for states to implement measures to prevent the proliferation of nuclear, chemical, and biological weapons. The FATF began addressing proliferation financing in 2007, recognizing its link to terrorism and terrorist financing.

The connection between proliferation and terrorism is critical, as the financing of WMD proliferation can support terrorist activities. Disrupting the flow of funds for proliferation is essential for preventing acts of terrorism.

The mechanisms used for financing proliferation often overlap with those used for terrorist financing. Therefore, the measures applied to combat proliferation financing are frequently similar to those used to counter terrorist financing.

PURPOSE OF THE POLICY

Since the Company is not registered as a bank or financial institution and is therefore not legally required to fully comply with the regulations governing these entities, the Company's owner and executive team recognize the importance of following best practices in financial compliance. This approach helps mitigate potential risks, ensures the Company maintains a strong reputation, and aligns with international standards. As a result, relevant provisions from the applicable regulations and legislation have been voluntarily incorporated into the Company's Anti-Money Laundering, Terrorist Financing & Financial Proliferation (AMLTF&FP) Policy and procedures.

As a reporting entity, the Company has the following key obligations:

- To know its clients and assess the risks associated with money laundering or terrorist financing.

- To report suspicious transactions, in line with the requirements set out in the applicable regulations.
-

2. MONEY LAUNDERING AND TERRORIST FINANCING RISKS FOR ONLINE GAMBLING OPERATORS

As an online gambling operator, the Company is exposed to a variety of risks related to the potential misuse of its services for money laundering (ML), terrorist financing (TF), and proliferation financing (FP). While these risks are inherent and cannot be fully eliminated, the Company believes that effective implementation of AMLTF&FP procedures, systems, and personnel can help identify and mitigate them.

Key Money Laundering and Terrorist Financing Risks Identified by GLADIA N.V:

Customer Identity Concealment

Risk of accepting customers who hide their true identity or address to mask illicit activity (e.g., multiple passports, synthetic identities).

Funds from Illicit or Terrorist Sources

Risk of unknowingly accepting deposits linked to illegal activities or terrorist financing, particularly from high-risk jurisdictions.

Unintentional Financial Channel for Illicit Funds

Risk of facilitating illicit fund movement where deposits are not used for gambling but temporarily parked in the system.

Illegitimate Withdrawals

Risk of customers withdrawing funds without engaging in actual gambling, potentially laundering illicit money.

Unintended Financial Institution-Like Activities

Risk of the Company unknowingly conducting activities outside its remit, such as storing, exchanging, or transferring customer funds for illicit purposes.

Specific Risks to the Company as a Online Gambling Operators

Bonus Abuse and Laundering via Bonus Schemes

Criminals may exploit bonuses to deposit illicit funds, fulfill wagering requirements, and withdraw “clean” money.

Multiple Account Creation

Risk of customers using fake or synthetic identities to create multiple accounts to launder funds through the platform.

Payments from High-Risk Jurisdictions

Risk of accepting payments from jurisdictions with weak AML/CTF controls or those under FATF sanctions, possibly linked to illicit activity.

Use of Anonymous Payment Methods

Risk of customers using prepaid cards or cryptocurrencies to deposit funds without revealing their identity, facilitating money laundering.

Unusual Betting Patterns

Large, unusual bets placed with no intent to win may indicate money laundering, where the goal is to transfer illicit funds, not gamble.

Rapid Withdrawals and Fund Transfers

Risk of funds being quickly deposited and withdrawn without gambling activity, suggesting money laundering.

Involvement in Gambling Syndicates

Risk of unknowingly being part of organized gambling rings used for laundering criminal proceeds.

Third-Party and Affiliate Risks

Third-party affiliates or agents may be involved in fraudulent or money-laundering activities to attract players, posing additional risks.

Cryptocurrency Use for Anonymous Gambling

Accepting cryptocurrency could facilitate anonymous transactions, making it difficult to trace illicit funds and increasing the risk of money laundering.

Mitigating Unidentified Risks:

In addition to the risks outlined above, the Company recognizes that there may be other, unknown sources of ML, TF, and FP threats. While fully identifying and preventing such threats may be beyond the Company's current capacity, management believes that fostering a culture of vigilance, risk awareness, and constructive skepticism among employees is the best preventive measure. Encouraging employees to remain alert and proactive is essential in identifying suspicious activities before they materialize into actual risks.

Integrated Risk Assessment Approach

Management understands that money laundering, terrorist financing, and business risks are closely interconnected. As a result, assessing these risks is an integral part of the Company's regular, systematic risk assessments. This ensures that potential MLTF&FP risks are continuously monitored and addressed within the broader context of the Company's overall risk management strategy.

3. CONTROL ENVIRONMENT

BUSINESS RISK ASSESSMENT

This Business Risk Assessment (BRA) evaluates the risks of money laundering (ML) and terrorist financing (TF) specific to the online casino and online sports betting operations of GLADIA BV. The goal is to identify and assess the potential risks these business activities pose and ensure that appropriate risk mitigation measures are in place to comply with applicable EU Anti-Money Laundering Directives (AMLD), national regulations, and best practices. This assessment also seeks to ensure that our operations are protected from being exploited for illicit financial activities.

Scope of the Business Risk Assessment

The Business Risk Assessment covers all online gambling operations, including:

- Online Casino (slot machines, table games, live dealer games).
- Online Sports Betting (betting on sports events, virtual sports).
- Payment Methods (e-wallets, bank transfers, credit cards, prepaid cards, cryptocurrencies, etc.).

- Customer Risk (assessing different types of customers based on profile, transaction patterns, and location).
- Third-Party Relationships (payment processors, affiliates, third-party platforms).

GENERAL ASPECTS OF MLTF&FP RISK ASSESSMENT

The risk assessment has the role of preventing the use of the Company by the clients in MLTF&FP activities or in activities that contravene the regime of international sanctions. In addition, the risk assessment allows the Company to determine the KYC measures that will be applied both in the procedure for the identification of a client, as well as during the Business Relationship, both for new clients and for the existing ones.

Risk assessment process for MLTF&FP threats is arranged along two different dimensions – nature and complexity of the risk; and value of the risk.

Along the first dimension, there are a number of risk triggers that allow for identification of the nature and complexity of the risk, i.e., citizenship of the player, changes in the registration information, e wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the MLTF&FP risk is simple or complex in nature. Relative simplicity or complexity further determines the Company's response and mitigation measures towards the risk.

Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific MLTF&FP risk. For example, the first deposited amount from a new client is usually accepted at the lowest allowable threshold, thus containing the MLTF&FP risk of improper use of the Company's Customer account for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the values of allowable deposits and withdrawals. Gradually, the Company's relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Risk Categories and Assessment Methodology

To assess the risks, we categorize potential risks into the following key areas: Customer Risk, Product/Service Risk, Channel Risk, Transaction Risk, and Operational Risk. Each category is evaluated using a Risk Matrix, which considers the following dimensions:

Likelihood: The probability that a particular risk could materialize.

Impact: The severity or potential consequence of that risk should it occur.

Velocity: The speed at which the risk can escalate or cause harm once it materializes.

Detectability: The likelihood of detecting the risk before it causes significant damage or harm.

Risk Level	Likelihood	Impact	Velocity	Detectability
Low Risk	Unlikely	Low Consequence	Slow	Easily Detectable
Medium Risk	Possible	Moderate Impact	Moderate	Moderately Detectable
High Risk	Likely	Significant Impact	High	Difficult to Detect

By considering these factors, the Company can categorize risks comprehensively and assign the appropriate level of monitoring and mitigation.

Risk Dimensions in Details

Likelihood

The likelihood refers to how probable it is that a risk will materialize. This is based on historical data, industry trends, and the nature of the customer's activities. For instance, customers from jurisdictions with known high levels of financial crime are more likely to present a higher risk.

Impact

The impact of a risk evaluates the consequences should the risk materialize. High-impact risks, such as large-scale money laundering or terrorist financing, can damage the Company's reputation, result in legal consequences, and expose the business to regulatory sanctions.

Velocity

Risk velocity measures how quickly a risk can escalate once it occurs. Certain risks, such as large-scale fraud or suspicious transaction activities, can spread quickly through the system and potentially result in severe financial damage. In contrast, other risks, such as slow changes in customer behavior or financial irregularities, may take longer to develop and require ongoing monitoring.

Detectability

Risk detectability refers to how easily a risk can be identified or prevented. Some risks, such as transactions that don't match the customer's typical behavior, are relatively easy to detect. Others, such as complex layering schemes in money laundering, may be harder to identify without sophisticated systems and increased vigilance.

GENERAL ASPECTS OF MLTF&FP RISK ASSESSMENT

The risk assessment has the role of preventing the use of the Company by the clients in MLTF&FP activities or in activities that contravene the regime of international sanctions. In addition, the risk assessment allows the Company to determine the KYC measures that will be applied both in the procedure for the identification of a client, as well as during the Business Relationship, both for new clients and for the existing ones.

Risk assessment process for MLTF&FP threats is arranged along two different dimensions – nature and complexity of the risk; and value of the risk.

- Along the first dimension, there are a number of risk triggers that allow for identification of the nature and complexity of the risk, i.e., citizenship of the player, changes in the registration information, e wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the MLTF&FP risk is simple or complex in nature. Relative simplicity or complexity further determines the Company's response and mitigation measures towards the risk.
- Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific MLTF&FP risk. For example, the first deposited amount from a new client is usually accepted at the lowest allowable threshold, thus containing the MLTF&FP risk of improper use of the Company's Customer account for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the

values of allowable deposits and withdrawals. Gradually, the Company's relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Risk Assessment and Classification

Based on the Risk Matrix dimensions outlined above, the Company will classify risks into one of the following categories:

- **Low Risk:** Risks that are unlikely to materialize or have minimal impact and are easy to detect and manage.
- **Medium Risk:** Risks that have a moderate likelihood of materializing or present moderate impact. They require routine monitoring.
- **High Risk:** Risks that are likely to materialize and may have significant impact, with potential for rapid escalation. These require enhanced scrutiny and mitigation strategies.

Actions Based on Risk Classification

The Company takes a differentiated approach to managing risks associated with Money Laundering and Terrorist Financing (MLTF&FP). Based on the risk classification of each customer, specific actions are taken to ensure compliance with AMLTF&FP procedures. The following key factors are considered when assessing a client's MLTF&FP risk:

Purpose of initiating the relationship: The nature of the customer's engagement with the Company.

Size and frequency of transactions: The volume, regularity, and value of financial activities conducted by the customer.

Duration and regularity of the Business Relationship: How long the customer has been with the Company and the consistency of their activity.

Regulatory and sector-specific guidelines: Applicable industry and legal standards to ensure the Company stays compliant.

Low Risk

For customers classified as low risk, the Company will rely on routine KYC procedures and ongoing transaction monitoring. While monitoring remains in place, no immediate intervention is typically required.

Actions:

Basic verification checks are performed during onboarding.

Standard monitoring of transactions to ensure consistency with the customer's profile.

No additional verification steps unless unusual activity is detected.

Medium Risk

Customers in the medium risk category are subject to enhanced monitoring. This includes more detailed transaction reviews and, when necessary, requesting further information to verify the customer's activities.

Actions:

Enhanced due diligence (EDD) processes are initiated if any irregularities arise.

Additional documentation may be requested, including evidence of source of funds or business operations.

Unusual or suspicious transactions are flagged for further investigation and potential escalation.

A more detailed review of the customer's transaction history and business activities.

High Risk

For customers identified as high risk, the Company will apply Enhanced Due Diligence (EDD) measures. These customers will undergo more frequent checks, with deeper scrutiny of their source of funds, business operations, and transaction patterns. Transactions exceeding certain thresholds will be manually reviewed, and withdrawals may be delayed pending further verification.

Actions:

In-depth investigation into the customer's source of funds and business background.

Frequent checks and closer monitoring of all transactions.

Manual review of any large, irregular, or complex transactions.

Delays in processing withdrawals, especially for transactions that are not aligned with the customer's typical behavior.

Enhanced monitoring of high-value transactions, especially those originating from or destined for high-risk jurisdictions.

Continuous review of the relationship to assess whether the customer should remain in the high-risk category or be reclassified.

In all cases, the Company's Compliance Officer (CO) and other relevant employees will ensure that the appropriate AML and KYC measures are followed based on the risk classification of the client. The goal is to maintain a proactive approach to managing MLTF&FP risks while providing a safe and compliant gambling environment.

MLTF&FP RISK ASSESSMENT

Risk assessment process for MLTF&FP threats is arranged along two different dimensions – nature and complexity of the risk; and value of the risk.

Along the first dimension, there exist a number of risk triggers that allow for identification of the nature and complexity of the risk, i.e. citizenship of the player, changes in the registration information, e-wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the MLTF&FP risk is simple or complex in nature. Relative simplicity or complexity further determines the Company response and mitigation measures towards the risk.

Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific MLTF&FP risk. For example, the first deposited amount from a new customer is usually accepted at the lowest allowable threshold for a given jurisdiction thus containing the MLTF&FP risk of improper use of the Company's Client account facilities for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the values of allowable deposits and withdrawals. Gradually, the GLADIA N.V relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Based on the dimensions described above, a specific MLTF&FP risk is classified as being high or normal; depending on classification, different actions are called for from the MLRO and other employees involved in MLTF&FP controls. Typical actions for high-risk detection situations are increase in the time lag for withdrawals and acceptance of the customer funds and enhanced verification of the customer.

INDICATIONS OF SUSPICIOUS, COMPLEX OR UNUSUAL TRANSACTIONS. OTHER RISKS

When performing the risk assessment of the clients, the Company will also take into account some risk hypotheses / indications which may lead to the recognition of suspicious, complex or unusual transactions or other risks in terms of MLTF&FP according to the AML Instructions and as identified by the Company:

1. Potential complicity of employees;
2. Use of false or stolen identity documents by players;
3. Concealment of the identity of the Beneficial Owner;
4. Lack of appropriate KYC policies;
5. Accessing multiple gaming platforms or collections of games within the same platform;
6. Complicity in the provision of bonuses or other benefits;
7. The vulnerability is associated with the ability of clients to join the game and deliberately transfer funds ("chip dumping");
8. E-Wallet, being considered a payment method that makes difficult for the operator to identify the source of funds;
9. Remote gambling used as a front for cash deposits, which are then transferred to bank accounts, with apparent winnings from gambling as the source of funds;
10. Transactions that appear to have no obvious economic or legal purpose.
11. Transactions that present an unusual or complex pattern compared to the client's risk profile or the pattern of transactions associated with the client, similar products or services;
12. Transactions in excess of normal limits typical for a player. An example would be an attempt to withdraw the funds from the gaming account in small instalments but totalling the entire balance of the account during a short period of time;
13. High turnover financial transactions (deposits and withdrawals) unwarranted by the gaming activity of the player;
14. Transactions outside of the player's regular payment and withdrawal patterns. An example is a series of minor deposits followed by no-activity period and a subsequent request for withdrawal of the entire amount;
15. The customer requests unnecessary or unreasonable levels of secrecy. For example, the client is reluctant to share due diligent information, or he appears to want to disguise the true nature of his business;
16. If the customer's or Beneficial Owner's source of wealth or source of funds cannot be easily explained;

17. Transactions of the customer, who has a political connection, or any other relevant links to a PEP or a Family member of PEP or Persons known to be close associate of PEP (persons who may abuse, directly or indirectly, of a public position for private gain), if such connection/link becomes known to the Company;
18. The customer insists that the transfer of earnings be made to the account or in the name of another person; Customers who constantly play against each other;
19. Clients who carry out transactions that appear to be disproportionate compared to the financial situation or income proven according to the documents certifying the source of the funds.

The Company recognizes that in addition to the indications of risks listed above there may exist various other unforeseen MLTF&FP risks. While prior identification of all such risks is not possible, the Company believes that fostering the general alertness, risk awareness and the spirit of constructive skepticism among employees are the best general preventive measures that could help timely identification recognition of suspicious transactions in terms of MLTF&FP risks.

In general terms, the Company will examine the context and purpose of all transactions that meet at least one of the following conditions:

1. are complex transactions;
2. are transactions with unusually high values;
3. do not fit into the usual pattern (taking into account any reasonable or justified deviations from the pattern);
4. do not have an obvious economic, commercial, or legal purpose.

In any of these cases, the Company will increase the degree and nature of the monitoring of the Business Relationship in order to determine whether such transactions or activities are suspicious. The identification of an isolated risk factor does not automatically determine the classification of a client in a higher or lower risk class. For each client, the Company will evaluate the risk factors presented in this Policy to establish the degree of risk, which will be established as a result of the logical combination of the identified risk factors. The placement of a client in one of the risk categories can be changed at any time during the Business Relationship as a result of obtaining new information by the Company. If the client is subsequently placed in a higher risk category, the Company will apply the appropriate KYC measures.

Also, the identified risk factors/ indications and their evolution will be continuously monitored by the compliance officer to determine the need to update the risk assessment section of this Policy.

Monitoring and Updating the Risk Assessment

The Company will continuously monitor risk factors and update the risk assessment accordingly. Changes in a customer's behavior, a shift in geographical risk, or the emergence of new money laundering techniques will all trigger an update to the risk classification.

If a High Risk classification is assigned later in the Business Relationship, the Company will apply enhanced KYC and AML controls. Additionally, any indications of suspicious activities will be investigated immediately.

AMLTF&FP DESIGNATED OFFICER

MLRO has working knowledge of the Company business environment, risks inherent to the Company's business model and AMLTF&FP provisions as stipulated in the Regulations as amended. AMLTF&FP Compliance Officer also performs the duties of Money Laundering Reporting Officer at the Company and is responsible for reporting transactions suspicious from AMLTF&FP standpoint to FIU Curacao.

General duties of the AMLTF&FP Compliance Officer include monitoring of the Company's compliance with the AMLTF&FP obligations, assessment of the business risks both internal and external, oversight of the AMLTF&FP related communication and training for employees, and reporting of the findings and critical issues of the AMLTF&FP systems and procedures to the managers and executives of the Company. The AMLTF&FP Compliance Monitoring Officer/MLRO ensures that the Company keeps and maintains all required AMLTF&FP records and that Suspicious Activity Reports are filed with FIU Curacao when required and appropriate.

The AMLTF&FP Compliance Officer is vested with full responsibility and authority to enforce the Company's AMLTF&FP Policy and working procedures. Responsibilities of AMLTF&FP Compliance Officer includes:

- Spearheads the global AMLTF&FP drive and is responsible for the overall AMLTF&FP strategy and policies of the Company.
- Conducts escalation and sanctioning in cases of internal non-compliance or lack of quality with AMLTF&FP strategy and policies.
- Represents AMLTF&FP activities at the senior management level.
- Manages central AMLTF&FP function and controls adequacy of policies, organizational structure and resources devoted to AMLTF&FP compliance.
- Drives communication to the senior management and other stakeholders with respect to issues concerning AMLTF&FP compliance.
- Maintains relationships between AMLTF&FP function and external auditors, regulators and other compliance authorities.
- Oversees and presents to the senior management overview and budget of the AMLTF&FP activities on a yearly basis.
- Contributes to the elements of the IT-systems related to AMLTF&FP compliance. - Presents to senior management the yearly AMLTF&FP Compliance Report.
- Reports to senior management all cases of non-compliance or inadequate compliance with AMLTF&FP policies and procedures on ongoing basis, together with recommendations for improvement.

4. CUSTOMER DUE DILIGENCE

Customer Due Diligence Measures and Regulatory Compliance

The Company ensures that robust Customer Due Diligence (CDD) measures are in place to mitigate risks associated with money laundering, terrorist financing, and fraudulent activities. CDD procedures are implemented in the following circumstances:

- Establishing a Business Relationship: CDD begins from the registration stage when initiating a business relationship with a client. This includes verifying identity, obtaining relevant documentation, and conducting initial risk assessments.

- Transaction Monitoring (Threshold-Based Due Diligence): CDD measures are triggered when transactions meet or exceed EUR 2,000. This applies to:
 - a) The collection of winnings
 - b) The wagering of a stake

A combination of the above in a single operation or multiple linked operations Transactions are deemed linked if they are executed by the same customer within the same game or gaming session.

Suspicious Activity Indicators: Regardless of transaction value, enhanced scrutiny is applied when there are indications of money laundering or terrorist financing. These include unusual transaction patterns, large cash deposits, or inconsistencies in customer behavior.

Verification of Customer Information: If there are doubts about the validity, accuracy, or adequacy of previously obtained customer identification data, the Company initiates a reassessment and requests updated documentation.

Know Your Customer (KYC) Process

The KYC process is a fundamental component of AML compliance, ensuring that all customers are properly identified and monitored throughout their relationship with the Company. The process consists of several key stages:

Identity Verification: Customers must provide valid government-issued identification documents, such as:

- a) Passport
- b) National ID card
- c) Driver's license
- d) Residence permit (for non-citizens where applicable)

Address Verification: Proof of residence is required to ensure that the customer's registered address is legitimate. Accepted documents include:

- a) Recent utility bills (issued within the last three months)
- b) Bank or credit card statements
- c) Official government correspondence

Source of Funds and Wealth Assessment: To determine the legitimacy of a customer's financial activities, the following information may be required:

- a) Proof of income (e.g., salary slips, tax returns, or bank statements)
- b) Business ownership documents (for self-employed individuals)
- c) Investment or property ownership documentation

Ongoing Customer Monitoring: The Company continuously reviews transaction behaviors to detect irregular patterns, such as:

- a) Frequent large deposits or withdrawals
- b) Rapid movement of funds across multiple accounts
- c) Unusual gaming or betting patterns
- d) Discrepancies between declared income and transaction volume

Risk Profiling: Customers are categorized based on their risk levels:

- a) Low-Risk Customers: Standard due diligence applies, with periodic reviews.

- b) Medium-Risk Customers: More frequent monitoring is required.
- c) High-Risk Customers: Enhanced due diligence (EDD) procedures must be followed.

Enhanced Due Diligence (EDD) Measures

EDD is conducted in cases where higher risks of financial crime are identified. This includes situations involving:

- Politically Exposed Persons (PEPs)
- High-value or high-frequency transactions
- Customers from high-risk jurisdictions
- Clients exhibiting unusual financial behavior

The EDD process consists of:

In-Depth Customer Review: Additional information is required, including:

- Multiple identity verification documents
- Proof of wealth and source of funds
- Personal interviews (if necessary)

Transaction Justification: Customers may be asked to provide supporting documents or explanations for specific transactions.

Ongoing Enhanced Monitoring: High-risk customers are continuously monitored using:

Automated transaction alerts

Periodic account reviews by compliance officers

Heightened scrutiny on changes in account activity

Approval from Senior Management: Establishing or maintaining a business relationship with a high-risk customer requires explicit approval from senior management.

Verification Methods

The Anti-Fraud Department utilizes multiple verification techniques to ensure compliance:

Automated Verification: AI-driven systems conduct preliminary due diligence by verifying documents, cross-referencing databases, and flagging inconsistencies.

Manual Review: Compliance officers conduct detailed reviews for complex cases, ensuring accuracy and regulatory adherence.

Electronic Registers: All verification data is securely stored and regularly updated for compliance audits.

PEP and High-Risk Customer Management

For transactions or business relationships involving PEPs, the following additional due diligence measures are applied:

Risk Management Systems: The Company maintains sophisticated risk assessment frameworks to detect PEP involvement.

Senior Management Approval: Establishing or continuing business relationships with PEPs requires written approval from senior management.

Source of Wealth and Funds Verification: PEPs must submit detailed supporting documentation verifying the legitimacy of their funds.

Ongoing Enhanced Monitoring: Transactions involving PEPs are continuously reviewed to detect any suspicious activity.

Reputation Assessment: The Anti-Fraud Department collects and verifies reference letters and third-party reports to evaluate a PEP's background and financial history.

Operational Responsibility and Compliance Framework

The Factoring and Monitoring (Anti-Fraud) Department is responsible for all due diligence processes. To maintain regulatory compliance, the department:

- Implements a risk-based approach in assessing financial crime risks
- Conducts periodic internal audits and updates due diligence procedures
- Trains employees on AML compliance, fraud detection, and regulatory changes
- Maintains comprehensive records of due diligence activities for regulatory reporting
- Technology and Human Oversight Integration

To enhance AML compliance, the Company employs a combination of:

Automated Systems: AI-powered transaction monitoring, machine learning algorithms for risk assessment, and real-time alerts for anomalies.

Human Review: Compliance officers manually assess flagged transactions, make informed risk judgments, and escalate cases when necessary.

By integrating regulatory compliance, advanced monitoring technologies, and a proactive risk-based approach, the Company ensures robust financial crime prevention while maintaining transparency and integrity in all customer interactions.

CONFIRMATION OF ULTIMATE BENEFICIAL OWNER OF THE FUNDS

The ultimate purpose of procedures for monitoring AML-TF compliance is to prevent the operation, under the guise of ordinary players and on the Company's platform, of the individuals related to or involved in moneylaundering and terrorist funding activities. Establishment of the identity of the ultimate beneficial owner of the funds is thus the key purpose of the AML-TF controls at the Company. The Company sets up a

number of barriers to prevent the suspect individuals from access to the Company's legitimate services: credit card verification; denial of service to the customers using someone else's credit cards; single-currency settlement; withdrawal identity verification and many others. There are also delegated responsibilities – for example, for the e-wallets originated deposits, responsibility for customer verification and funds provenance lies with e-wallet.

IDENTIFICATION AND VERIFICATION SYSTEMS

The Company's identification and verification systems are predominantly computer-based and include various data-bases, data-mining facilities and cross-checking software. The products of third-party providers such as KYCAid, credit-card databases and other sources are utilized in order to control the customer identification and fund-origination risks. The Company's accounting system traces the account movements by individual IP address of the players. List of IP addresses is stored and can be viewed for each game account; all IP addresses are also stored in the logs of the program (including archived). The system has a viewing facility for analysis of a list of players and the number of movements at the specified IP address. Recording of IP addresses allows to track down fraudsters whose activities are connected with gaining access to other customers' player account or gaining possession of their funds (an example of indication to a possible theft of credit card is Cyprus-originated and t: if BIN code of a credit card used by a player, the IP address of the gaming account is identified as Nigerian. If such a combination occurs, the account is immediately blocked until the owner passes the full verification).

EMBARGO REQUIREMENTS FOR MLTF&FP CONTROLS SPECIFICALLY CONCERN TWO COUNTRY GROUPS:

- the US List of State Sponsors of Terrorism¹. Currently the list includes Cuba, Iran, Sudan and Syria. - the countries and territories with prohibitive and internationally promulgated territorial gambling regulations. Currently the list includes the USA and its dependencies, Israel, France, UK and outlying

Requests from potential customers from the aforementioned countries and territories (residential addresses and IP addresses) are denied. Furthermore, the names of such customers are retained on record, blacklisted and are routinely screened in any future customer requests.

¹ <http://www.state.gov/j/ct/rls/crt/2012/209985.htm>

Sanctions requirements for MLTF&FP controls:

Sanctions Compliance and Financial Sanctions

Targeted financial sanctions require countries to freeze funds and assets, ensuring that no funds or other assets are made available—directly or indirectly—to or for the benefit of any designated persons or entities. All natural and legal persons in Curaçao are required to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This is in compliance with United Nations Security Council (UNSC) resolutions and the Common Foreign and Security Policy (CFSP) of the European Union (EU).

Compliance with sanctions imposed by the UNSC is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao under the Kingdom Sanctions Act. Additionally, the following sanctions bodies play a critical role in imposing financial sanctions:

United Nations (UN): The UN imposes financial sanctions through resolutions passed by the UN Security Council. Member states are required to implement these sanctions in their domestic laws and regulations.

European Union (EU): The EU enacts financial sanctions based on decisions within the Common Foreign and Security Policy framework. These sanctions include asset freezes and restrictions on financial transactions with specific individuals, entities, and countries.

Office of Foreign Assets Control (OFAC): The U.S. Department of the Treasury administers and enforces sanctions through OFAC, targeting foreign countries, regimes, terrorists, and international narcotics traffickers based on U.S. foreign policy and national security interests.

Her Majesty's Treasury (HMT), United Kingdom (UK): The UK imposes financial sanctions, implemented through statutory instruments and primary legislation. These sanctions cover a broad range of individuals, entities, and sectors in countries that threaten UK national security or foreign relations.

Sanctions Procedures and Obligations

To comply with the relevant sanctions, the company undertakes the following measures:

Risk Assessment: Before undertaking any commercial transactions with clients, providers, or partners, the company seeks to understand the risks and relevant aspects of the transaction to identify potential Red Flags.

Sanctions Due Diligence: Ensure that sanctions due diligence is conducted in accordance with applicable regulations.

Sanctions Lists Screening: The company ensures that it does not engage with clients, providers, or partners listed as sanctioned entities or individuals in the sanctions regulations imposed by the UN, EU, OFAC, and HMT.

Immediate Suspension: Activities are immediately suspended if there are Red Flags regarding potential sanctions violations.

Contractual Assurance: Ensure that all clients, providers, and partners represent in contracts that they are not subject to sanctions and will not engage in activities that violate the sanctions.

Ongoing Monitoring: Continuously monitor for Red Flags throughout the business relationship to ensure ongoing compliance.

Monitoring Sanctions Compliance

Monitoring sanctions compliance is an ongoing process that is integral to the company's internal controls. The following steps are undertaken to ensure compliance with the relevant sanctions regulations:

1. **Sanctions List Updates:** The company regularly checks and updates its sanctions lists against those provided by the United Nations, European Union, OFAC, and HMT. This includes monitoring changes in the sanctions lists, such as additions, removals, and updates to the designation of individuals, entities, and countries under sanctions.
2. **Screening of Transactions:** All transactions, including payments, transfers, and business engagements, are screened against current sanctions lists to detect potential violations. Screening is automated through specialized sanctions screening software that matches transaction details against the sanctioned persons/entities.
3. **Real-Time Monitoring:** The company employs real-time transaction monitoring systems that flag suspicious or high-risk transactions linked to sanctioned entities or countries. These systems are configured to alert the relevant compliance team immediately for investigation.
4. **Risk-Based Approach:** The company adopts a risk-based approach to monitoring sanctions compliance, prioritizing higher-risk transactions or clients based on factors such as geography, industry, and historical association with sanctioned entities. Enhanced due diligence procedures are applied to transactions involving high-risk areas.
5. **Training and Awareness:** Staff are regularly trained on recognizing red flags related to sanctions violations. The compliance team is provided with ongoing education on the latest updates in

sanctions regulations and enforcement actions to ensure that they can identify emerging risks and trends.

6. **Audit and Reporting:** Regular internal audits are conducted to assess the effectiveness of the sanctions monitoring program. The results are reviewed by senior management, and any issues are addressed promptly.

The company also maintains reporting mechanisms for suspected sanctions violations, which are escalated to the relevant authorities when necessary.

Collaboration with Authorities: In cases where potential violations are identified, the company works closely with the relevant regulatory and law enforcement authorities to ensure appropriate actions are taken. This includes cooperating with national and international bodies to address potential risks.

Sanctions List - Targeted Countries and Entities

The following countries, territories, and groups have been subject to economic and trade sanctions imposed by international sanctions bodies:

Russia (Russian Federation)

Crimea (Ukraine)

Cuba

Iran

North Korea

Sudan

Syria

Libya

South Sudan

Venezuela

Belarus

Myanmar (Burma)

Zimbabwe

Afghanistan

Central African Republic (CAR)

SHELL COMPANIES AND MONEY LAUNDERING

Shell companies are corporations created to protect or hide the assets of another company. They only exist on paper and have no physical location, staff, revenue, or significant assets, but they may have bank accounts or investments. While shell companies can be created quickly and affordably in the legal, financial system to raise funds, hold stocks, or serve as limited liability trustees, they are not necessarily illegal. However, they are often used for unlawful purposes, particularly as part of money laundering



operations. Shell companies can be established by registered agents in most countries to hide Ultimate Beneficial Ownership (UBO). This means that shell companies can be set up with a level of secrecy and then used to conceal illegal funds, evade sanctions, and circumvent anti-money laundering (AML) measures used by companies to detect suspicious financial activity.

To effectively manage the AML risk associated with shell companies and adhere to domestic legislation and FATF guidelines, GLADIA N.V refrains from establishing any business relationships with such entities.

5. MONITORING

MONITORING OF THE ACCOUNT ACTIVITIES

This component is central to the Company's AMLTF&FP efforts. Account monitoring is conducted on the ongoing basis by the officers responsible for various operating aspects of the business. The deposit and withdrawal policies are enforced personally by CFO and MLRO. This enforcement is conducted daily and supported by various thresholds set up to flag the potential problems.

Overall, monitoring of account activities consists of:

- Monitoring of new registrations
- Monitoring of deposit activity
- Monitoring of gambling activity
- Monitoring of account access
- Monitoring of account detail changes
- Monitoring of withdrawal activity
- Monitoring of registration data to ensure it is kept up to date

Critical controlling measures with respect to MLTF&FP prevention are:

- denial of withdrawals for the inactive funds
- detection of the unusual payment patterns (i.e. deposit activity does not match the betting activity or large deposit movements unwarranted by the betting patterns)
- periodic screening of e-wallets used by the players
- pro-active recognition and prevention of players' fraudulent intentions or activities. This component is an indirect indication of probable MLTF&FP threats.

TRANSACTIONS MONITORING

Monitoring of monetary transactions is a constituent part of the monitoring of the account. Main purpose of transaction monitoring with respect to MLTF&FP threats is to identify and to prevent the suspicious transactions from taking place at the business facilities. Various safeguards and awareness triggers are employed in transactions monitoring e.g. absolute monetary limits; single-player-single-account, single-session and single-currency rules; obscure event bets.

Assignment of status (and color grades for visual recognition) to the players according to the types of games and gaming behavior:

- **No status:** players who have not triggered suspicions with any departments of the Company. Usually applied to new customers, which have not finished verification procedure yet. Limits could be set according to a governmental database of self-limited individuals from specific countries.

- **Monitored:** players who have gone through full verification (provided the passport data, etc.). The gaming activity of customers in this group was analyzed by the Anti-Fraud Department employees, no suspicious actions were detected at the moment.

- **Arbitrage:** players with the history of placing sure bets

- **Scammers**

- **Foreigners:** players whose country of residence is outside of the Company's core region of operations.

- **Suspicious:** gaming accounts placed under close monitoring by Payment and Factoring & Monitoring Departments

- **Potential VIP players**

- **Existing VIP players.** A group of players, which constantly place bets with amounts over 100 USD. Their gaming activity is not limited and they have higher priority in processing transactions.

For player, who has not pass verification procedure during first 30 days since initial registration, will be prohibited withdrawal of funds from the account. Placing deposits and betting activity allowed.

For player, who has not pass verification procedure after 30 days since initial registration, will be prohibited withdrawal of funds and betting activity. Placing deposits allowed. When trying to confirm a bet in the coupon, display a corresponding message in the channel in use.

if the player has a "good" category, it doesn't mean that he drops out of control. Payment and Factoring & Monitoring Departments carry out continuous monitoring of all players and transactions.

Employees of GLADIA N.V seeks to identify the following indications of the potential MLTF&FP threats:

- Individual or linked transactions which are complex or unusually large with no apparent or lawful economic purpose, including those relative to a relationship;

- Unusual patterns of transactions with no apparent economic or lawful purpose, including those relative to a relationship;

- Transactions which exceed certain limits with no apparent economic or lawful purpose, including those relative to a relationship;

- Very high account turnover inconsistent with the balance;

- Transactions which are outside of the customer's regular transaction activity.

Changes in registered players' information are monitored by Anti-Fraud Department; consistency and significance of changes are analyzed daily; game session patterns are matched against the historic average profile (its IP addresses, his types of games and style of bets, Payment Systems that he uses etc.) for a given game to ensure that, in each particular moment, they resemble the historic gambling trends for the customer. Significant deviations during game sessions are documented, analyzed and reported.

If any unusual behavior is identified by the employees of the Department, they make short time block of the activity on the customer's account in order to check whether the customer performs actions by himself and make investigation on player's activity.

As for the internal controls, Anti-fraud department on a daily basis generate Manual adjustment report and review any manual changes that were done to the client's account.

MONITORING OF HIGH-RISK CLIENTS

Suspicious players and scammers have the highest risk range of all players. There are several categories of such kind of players and the measures for their detection:

“Review”- this group includes players whose gaming activity is unusual. These accounts are limited by 5-10 USD bet amount or even blocked in order to prevent fraud. For the “Review” the account will be unblocked only when Anti-fraud or Payment or other departments who detected the trigger would confirm that the customer has passed all the required procedure.

“Betting arbitrage” - is an example of arbitrage arising on betting markets due to either bookmakers' differing opinions on event outcomes or errors. When conditions allow, by placing one bet per each outcome with different betting companies, the bettor can make a profit regardless of the outcome. Mathematically, arbitrage occurs when there are a set of odds, which represent all mutually exclusive outcomes that cover all state space possibilities (i.e., all outcomes) of an event, whose implied probabilities add up to less than 1.

“**Bonus hunting** (also known as bonus bagging)” is a type of advantage gambling where turning a profit from sportsbook bonus situations is mathematically possible.

“**Late Betting**”- players that place bets on the matches, which are finished already, but not included to the system, result. Also are detected by gaming patterns, by analyzing time of bets and real time of events happened. Depending on player's average bet amount the 1-20 USD limit in equivalent could be implemented.

“**SFM (Suspicion Fixed Matches)**” when player that often bets on events or leagues that are considered highly corrupt and with a high risk of negotiated matches.

“**PEP**” - Means a natural person who is or who has been entrusted with a prominent public function in the Republic or another country, a close family member of that persons as well as a person known to be a closely associated with such person. Transactions of PEPs continuously monitored, especially to ensure that the threshold has not been exceeded and that the amounts played correlate with the income profile of the PEP received during the Enhanced Due Diligence procedure.

Following databases are used for detection of high-risk players:

- KYCAid a database of Politically Exposed Persons (PEPs) and heightened risk individuals and organizations, used around the world to help to identify and manage financial, regulatory and reputational risk.
- United Bookmakers' databases which include a full list of fraudulent players
- Adverse media publications, publicly available registers etc.
- Payment systems database – reconciliation to the records of the customers.
- Anti-fraud and Payment departments often refer to the data provided by the Payment systems in order to reconcile information provided by the customer in his registration form with the information recorded in Payment System database. In the black-lists employees who

perform controls can find list of persons, which were blocked according to the certain reasons. And finally, Payment Systems send automatic or manual notifications, if they detect any suspicious transaction. All these notifications are checked and assessed by the Responsible employees.

After suspending the account, a notification appears on the customer's page and the Support Team requires information and/or documents in order to check the suspicious action. Also, additional information may be requested from affiliated who are processing deposits and withdrawals from the gaming accounts, in order to obtain information about the origin of the funds.

The customer still has the possibility to enter his personal account during the investigation process but the funds will remain frozen and all transactions blocked until the investigation is completed.

All the investigation steps recorded in the system. If it completed successfully, the responsible employee will unblock the account and the customer can manage his funds again. If there were no response to the notification or the customer provides not enough data to complete the investigation - the account will remain blocked until the requested documents received.

“Problematic Gamblers”- we characterize the players whose behavior is excessive and/or aggressive and in general problematic like harassing the support team staff or whose actions could be classified as compulsive gambling. There are 3 ways of identifying players who display problematic gambling behavior and the respective following steps for each type of it:

I. The customer informs the Support team by himself about his gambling problem through e-mail or chat or telephone. The request can include limits of bets that should be set to the customer OR temporary blocking of the account. After the Anti-fraud department execute the request, the customer notified about the changes done to his account via e-mail.

II. Mathematical review. One of the triggers that monitored by the department is the problematic gambling trigger. It includes the following algorithms: if a gamer has losses, which were increased 10 times during a period of more than 3 months (90 days) the gamer is identified as a problematic one OR if a gamer doubled his losses each month during the last 12 months he is identified as a problematic gambling customer. According to these analyses, the Support department initiates the communication with the customer, where they describe the situation, give links to gambling addiction help websites and propose measures to the customer like selflimitation with the most comfortable and suitable conditions.

III. Support team review. While communicating with the customers, the Support department identifies the problem gambling customers if their chats or calls are harassing to the Support team or other customers or compulsive gambling. One of the main triggers of the compulsive gambling is the constant request of the credit to be issued by the website. (no one can issue any credits to customers).

REPORTING SUSPICIOUS ACTIVITIES AND TRANSACTIONS

All suspicious activities and transactions are recognized and recorded in the system. All suspicious activities / transactions, including attempted transactions reported internally first. The officers responsible for respective areas of transaction monitoring report the suspicious activities to MLRO immediately upon identification, together with a brief description of specific mitigating measures taken. Such reporting is performed in both oral and written form depending on gravity of an incident reported.

The Company's general approach is to file the written report only in cases of reasonable suspicion of substantial violation of Regulations or substantial threat to the business. A degree to which a particular violation or threat is deemed "substantial" is left to the discretion of the officer in charge of specific controlling area and their respective upper management. Due to the fast-moving nature of the business, the management feels that this approach is fully justified.

Employees' may report a suspected instance of ML/FT to the MLRO even when their immediate superior is in disagreement with them. The MLRO must determine if the information available can be considered as sufficient for STR to be made to the FIU.

The format of the report on suspicious activities and transactions is provided in Appendix A.

6. EMPLOYEES

STAFF RELIABILITY AND PROBITY

The business of GLADIA N.V is an amalgamation of appropriately qualified people and past-paced technological innovation. Employees are one of the most valuable assets and a critical component of the Company's operating model. In an intense, gain-driven betting environment, staff reliability and probity is of paramount importance to an extent unseen in other businesses.

The Management of GLADIA N.V recognizes this and, therefore, the employees are expected to:

- conduct their activities in accordance with direct instructions of the immediate supervisors - exercise sound judgment in situations requiring initiative and unsupervised decision-making - behave ethically towards the company, colleagues, clients and third parties

- be fair, honest, dependable and accountable in business dealings

- avoid business and personal actions that might cast appearance of impropriety or ethical ambiguity - comply with the respective HR policies and regulatory requirements

- declare any actual or perceived conflicts of interest as soon as such conflicts become known - maintain confidentiality and prevent the disclosure of the confidential information - refrain from accepting inducements, incentives, gifts or other benefits from the colleagues and third parties

that may lead to, or may be seen as leading to, an unfair advantage to third parties or to unfair treatment of the business

- communicate internally and with the third parties using clear and concise meanings, in a timely manner and via the established communication channels

- decline invitations from the mass media and the Internet-based platforms (forums, info-aggregators, news originators and others) to discuss the Company's business.

SCREENING

The company developed and supports the HR and control policies and procedures for effective initial screening of candidates and subsequent dealings with employees:

- All personnel undergo the initial procedure for personal identification.

- During the first interview, all candidates are required to complete the ID profile designed by HR Department. The ID profile includes a number of psychological tests designed to determine whether a candidate might inflict, under certain conditions, harm to the company.

- Upon completion of the ID profile and analysis by the HR Department, the recruiter conducts initial interviews with the candidates using a number of further psychological tests.
- Following the conclusion of the initial interview, the second interview by HR Director is conducted for the successful candidate.
- The next step in the hiring process is a conversation with the subject area manager, followed by the meeting with a member of the internal security department.
- Conduct, by a member of internal security department, of the background check on the candidate including, but not limited to, communication with the previous immediate supervisor of the job candidate; verification of the criminal record; examination of job references and communication with the sources; search in the open public sources and the Internet.

Having succeeded in the screening process in its entirety, the new employees are given the mandatory introductory course in their respective areas for three weeks and have to pass the exams as follows.

Stage 1: Employee adaptation and lectures on the bookmaking basics. Exam.

Stage 2: Lectures on the payment systems. Exam and issuance of the internal certificate. Stage 3: Learning how to work with the software. Exam.

Stage 4: Lectures on dealing with customer complaints.

Stage 5: Training at the workplace and a final exam.

After successful completion of all five stages, the employee commences the duties in probation mode under close supervision of a member of the internal security department and the direct area manager.

For the candidates applying to executive positions, the hiring procedure involves a mandatory personal conversation with the CEO upon which the final decision to hire is made.

PROFESSIONAL SUPPORT AND TRAINING

The company supports professional efforts by its employees to remain at the forefront of the best practice and technological innovation in the e-gambling and betting industries. It is recognized that such support may take several forms including but not limited to the on-site and distance training, ad-hoc working groups, technical and situational seminars and some others.

The company offers training courses and conducts a series of seminars for the employees in the varied subject areas of direct interest to the business.

Trainings in Business Administration are conducted for managers of the company, which include five main blocks: building of the management platform, forming the levers of managerial effectiveness, integration of the management skills, the development of business in the global sphere, and also training courses of business English are conducted for all employees of the company.

Professional upgrade courses are conducted internally for the staff of Trading and Operational Departments by the divisional heads and Directors of respective departments.

Marketing Department staff participates in various training conferences on various aspects of marketing, including the practice of e-mail marketing; SEO optimization, ICE Totally Gaming, web analytics, etc.

The Finance Department staff participate in training courses on the subjects of management accounting, budgeting and planning, internal controls, and management finance.

AML TRAINING

The MLRO is responsible for the conduct of the introductory AMLTF&FP training course for every new employee and the subsequent AMLTF&FP updates in the “what?” and “how to?” format including:

- what is the employee role in the Company’s compliance effort and how to perform the individual compliance duties
- what are and how to identify red flags and indications of money laundering that may arise in the course of the employee daily duties
- what to do once the risk is identified (including how, when and to whom to communicate the initial suspicion and how to escalate the level of awareness of the threat for further processing and analysis) - what are the latest tools, updates and improvements in the AMLTF&FP investigations.

The MLRO keep a register of all trained employees of the Company dealing with monitoring of transactions, engaged in the management of the company, any authorized representatives and/or responsible persons.

7. RECORD-KEEPING

A complete history of each player's account transactions starting from the date of account opening and to his latest bet is saved on the computer system.

The system keeps the following information:

Primary customer data (required at the registration stage) and scanned documents.

Comments by the employees of the respective departments concerning each player account. There are fields designated to comments in the program for four departments: Anti-fraud, Payments, VIP Players and Support. Each department provides comments (notes) in their respective fields only and strictly in accordance with their official duties. For example, the VIP Players Department usually provides ranking information of VIP players (ranked by stars: from a “small” VIP player to the largest according to graduation, etc.).

When the comments lose relevance with the passage of time, head of the appropriate department may remove a comment however the log will be kept on record indefinitely.

System also keeps records regarding profitability of each gaming account for the entire period of its existence – also utilized as an MLTF&FP risk trigger.

All suspicious activities and transactions are recognized and recorded in the system. Upon receipt of the Report on suspicious activities and transactions, MLRO decides as to the further course of actions concerning possible reporting of the transactions to authorities and licensing authority.

All transactions history of a player including amendments, additions and deletions to the transactions are kept for records for 5 years’ period. For customer due diligence data and information, the holding period is 5 years following the date of cancellation of customer relationships. Records are maintained on company servers and instantaneous back-up is performed.

The system provides technical facilities for sending the messages to clients; such messages are stored in a special

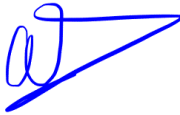
Gladia N.V.

Message Box in the context of each player account, as well as in the logs of the system. Disputes with the player arising in the gaming context are solved operationally by communicating with the customers via Skype, email, chat, or phone. The records of disputes are stored in the system.

8. RATIFICATION

The Policy will be valid for a period up to its annual or required reviewing.

In witness whereof, GLADIA N.V, has caused this Policy to be duly executed this day of May 13, 2025.



eMagnus Curacao B.V.
Managing Director



APPENDIX A. REPORT ON SUSPICIOUS ACTIVITIES AND
TRANSACTIONS

Date	Reporting officer	Description of suspicious activity or transaction	Area ²	Mitigation measures taken NO / YES – description	Comments
...	...	...	...	...	...
...	...	...	...	...	...
...	...	...	...	...	...

