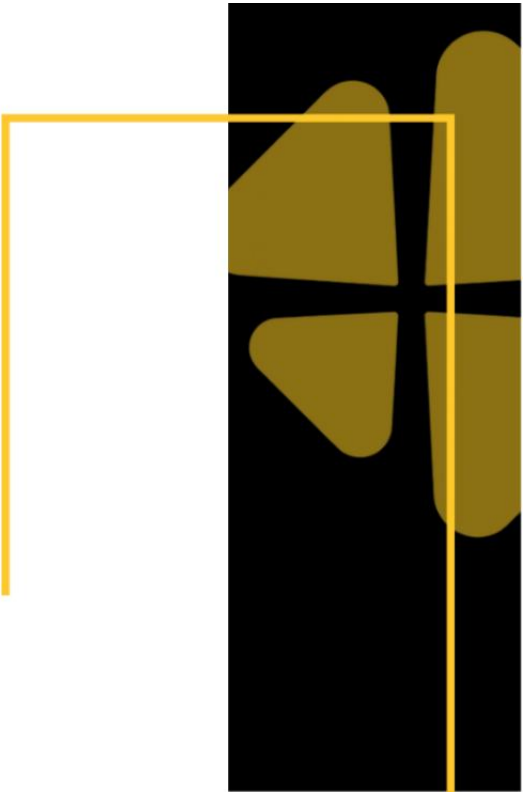




Anti-Money Laundering and Counter-Terrorism Financing Manual

- MIC Group Entertainment N.V -

Index

I. Introduction	4
II. Scope	4
III. Objectives	4
IV. Términos y Definiciones	5
V. Regulatory Framework	6
VI. AML/CFT Risk Prevention and Management Policies	6
VII. Training Programs	7
VIII. General Guidelines Established in the Site's Code of Conduct for Managing ML/TF Risks	7
IX. Violations and Internal Sanctions for Non-Compliance with AML/CFT Obligations ..	8
X. Functions and Responsibilities	8
10.1. General Obligations Applicable to All Employees in AML/CFT Prevention	8
10.2. Functions and Responsibilities in AML/CFT Risk Prevention and Management	9
10.3. Organizational Structure	10
XI. AML/CFT Risk Management Mechanisms	11
11.1. Description of ML/TF Risk Factors	11
11.2. Role of the Compliance Officer in Evaluating New Products and Markets	12
11.3. Methodology and Criteria for Customer, Supplier, and Counterparty Due Diligence	13
11.4. Background Screening of Employees and Management	13
11.5. Procedures for the Analysis of Alerts, Unusual Transactions, and Suspicious Activities	14
XII. Recordkeeping and Communication Procedures	14
12.1. Internal Communication Channels	14

12.2 Consultation Mechanisms between the Compliance Officer and Company Departments	15
XIII. International References and Regulatory Framework for AML/CFT Prevention	15
XIV. Enhanced Due Diligence (EDD).....	16
XV. Evaluación basada en riesgos	16
XVI Ongoing Monitoring.....	16

I. Introduction

The Anti-Money Laundering and Counter-Terrorism Financing Manual constitutes the institutional framework that guides the policies and procedures of the organization (hereinafter referred to as the Site), within the applicable regulatory context. Its purpose is to establish clear controls that enable operations to be conducted with integrity and transparency, preventing the Site from being used for illicit or unlawful purposes.

The structure of this document is based on a risk-based approach (RBA), which allows preventive measures to be adapted according to the characteristics and vulnerabilities of each process and operational unit. This approach strengthens the compliance culture, promotes shared responsibility at all levels of the organization, and reinforces the documentary traceability required to meet audit standards and regulatory requirements.

II. Scope

The Anti-Money Laundering and Counter-Terrorism Financing Manual applies to all operations and activities carried out by the Site. Its scope includes account opening and management, financial transaction handling, relationships with suppliers and counterparties, as well as any process that may involve exposure to ML/TF/PF risks.

The application of this manual extends to directors, managers, employees, users, and suppliers associated with the Site, all of whom must comply with the policies and procedures established herein. It also includes interactions with external entities that, due to the nature of their functions, may impact risk prevention.

The manual establishes a uniform framework that guides the actions of all parties associated with the Site and consolidates a comprehensive prevention system aligned with current regulatory requirements.

III. Objectives

The purpose of this manual is to establish an institutional framework that guides the Site's actions regarding money laundering and terrorism financing risks, ensuring that operations are conducted with integrity and transparency in accordance with applicable regulations and international standards.

It aims to consolidate a culture of compliance at all levels of the organization, promoting shared responsibility among management, employees, suppliers, and counterparties.

Additionally, it establishes risk monitoring and evaluation procedures to identify and mitigate threats that may compromise the Site's operations.

Another key objective is to strengthen staff training, ensuring that each member has the necessary knowledge to properly apply prevention policies and procedures.

IV. Términos y Definiciones

- **Senior Management:** Group of executives with strategic decision-making authority (may include the CEO and other senior roles).
- **Terrorism Financing (TF):** The act of providing funds or resources to support terrorist activities.
- **Proliferation Financing (PF):** The provision of financial or material resources to support the production, acquisition, or transport of weapons of mass destruction.
- **Financial Action Task Force (FATF):** An intergovernmental body established in 1989 to combat money laundering, terrorism financing, and other threats to the global financial system.
- **General Management:** The highest executive level responsible for operational leadership and implementing strategic decisions made by Senior Management.
- **KYC (Know Your Customer):** Procedures used to verify the identity of customers.
- **Money Laundering and Terrorism Financing (ML/TF):** Illicit activities aimed at disguising the illegal origin of funds and/or providing financial support to terrorism.
- **ML/TF/PF:** Acronym for Money Laundering, Terrorism Financing, and Proliferation Financing.
- **AML/CFT System (SPLAFT):** A set of policies and procedures designed to prevent misuse of services for illicit purposes.
- **Obligated Entity:** Any individual or legal entity required by law to implement prevention measures and report suspicious transactions to the FIU.
- **Suspicious Transaction:** Any activity that appears unusual, inconsistent, or lacks a clear lawful explanation.
- **Compliance Officer:** Individual responsible for implementing and overseeing AML/CFT policies.

- **Organization:** The formal structure of the company, including roles, responsibilities, and processes supporting AML/CFT compliance.
- **Politically Exposed Person (PEP):** Individuals with prominent public functions or close associations that increase risk exposure.
- **Regulation:** A set of rules issued by an authority to govern operations.
- **Site:** Refers to the website www.micasino.com
- **Financial Intelligence Unit (FIU):** Authority responsible for receiving and analyzing financial transaction reports to detect illicit activities.

V. Regulatory Framework

This framework is complemented by the international standards of the Financial Action Task Force (FATF) and the recommendations of the Financial Action Task Force of Latin America (GAFILAT), ensuring that internal policies and procedures remain up to date and aligned with international best practices in the management of risks related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

VI. AML/CFT Risk Prevention and Management Policies

The policies for the prevention and management of money laundering and terrorist financing risks constitute the institutional guidelines that direct the organization's actions in response to potential threats. These policies are conceived as general principles that must be observed at all levels of the Site and in each of its operations.

The Site adopts a policy of integrity and transparency, through which it commits to conducting its activities ethically and in accordance with applicable regulations, preventing its processes from being used for illicit purposes.

A shared responsibility policy is established, recognizing that the prevention of ML/TF is an institutional obligation involving directors, employees, suppliers, and counterparties, under the coordination of the Compliance Officer.

The Site maintains a continuous training policy aimed at strengthening staff competencies and consolidating a culture of compliance. Training programs are designed in accordance with the Financial Intelligence Unit (FIU) guidelines and international standards set by the FATF.

Finally, a policy of cooperation with competent authorities is defined, including the timely reporting of suspicious transactions, responsiveness to information requests, and collaboration in supervision and audit processes, thereby reinforcing document traceability and institutional responsiveness.

VII. Training Programs

The Site establishes training programs on the prevention of money laundering, terrorist financing, and proliferation financing. These programs constitute an essential component of the AML/CFT system (SPLAFT) and are aimed at strengthening the compliance culture at all levels of the Site.

The minimum training content includes the study of the applicable regulatory framework, internal prevention policies, procedures for the identification and due diligence of users and suppliers, transaction monitoring mechanisms, and reporting flows for suspicious activities. It also covers red flags and risk typologies, as well as the definition of roles and responsibilities of Senior Management, the Compliance and Monitoring Department, the Compliance Officer, and other areas involved in the system.

Training is delivered through various formats, including initial onboarding for new staff, periodic training with regulatory updates, specialized programs for critical areas, and technology-assisted learning methods. Each activity is documented through attendance records, materials used, and evaluations conducted, ensuring process traceability and compliance with the minimum requirements established by applicable regulations.

VIII. General Guidelines Established in the Site's Code of Conduct for Managing ML/TF Risks

The Site's Code of Conduct constitutes a reference framework that guides the ethical behavior of its members in relation to money laundering and terrorist financing risks. This document establishes guiding principles aimed at preserving institutional integrity and promoting a corporate culture aligned with regulatory requirements.

The general guidelines focus on the explicit prohibition of engaging in operations that may be linked to illicit activities, the obligation to act with transparency in business relationships, and the preservation of trust with users, suppliers, and authorities. The

Code establishes that all business decisions must consider exposure to ML/TF risks and adopt measures to reduce the possibility that internal processes may be used for improper purposes.

Additionally, the Code of Conduct establishes that the Site must promote responsible behavior in the management of sensitive information, preventing its misuse and ensuring that internal control processes are carried out with technical rigor and professionalism. The importance of corporate ethics is recognized as a cross-cutting element in risk prevention, ensuring that each member of the organization acts in accordance with institutional values and in compliance with the applicable regulatory framework.

IX. Violations and Internal Sanctions for Non-Compliance with AML/CFT Obligations

The Site establishes an internal audit and control system aimed at evaluating the effectiveness of the AML/CFT system (SPLAFT) and verifying the proper implementation of the policies and procedures defined in this manual. This system is conceived as a permanent supervisory mechanism that enables the identification of deviations, the proposal of corrective measures, and the strengthening of the compliance culture at all levels of the organization.

Internal audits are conducted periodically and cover critical processes, supporting documentation, and departmental reports. Findings must be submitted to the Board of Directors within thirty days following the annual closing, and the Annual Implementation Report must be submitted through the Compliance Officer.

Audit results are consolidated into reports that identify opportunities for improvement, define procedural adjustments, and strengthen preventive measures. In this way, the Site maintains a dynamic control system that adapts to regulatory changes and sector requirements, reinforcing the effectiveness of the AML/CFT system in addressing money laundering and terrorist financing risks.

X. Functions and Responsibilities

10.1. General Obligations Applicable to All Employees in AML/CFT Prevention

All employees of the Site, regardless of their position or function, are subject to general obligations regarding the prevention of money laundering and terrorist financing. These

obligations derive from both applicable regulations and the internal policies established under the AML/CFT system (SPLAFT), and constitute an institutional commitment involving every individual associated with the Site.

Employees must act with integrity and transparency in the performance of their duties, in compliance with the provisions set forth in this manual, the Code of Conduct, and the internal work regulations. They are also responsible for applying customer and supplier due diligence procedures, supporting transaction monitoring activities, and promptly reporting any unusual or suspicious activity.

Active participation in training programs is another essential obligation, ensuring that personnel maintain up-to-date knowledge of applicable regulations and international best practices. Likewise, employees must safeguard the confidentiality of sensitive information and contribute to the documentary traceability of processes, ensuring that the Site's activities are conducted in accordance with the regulatory framework.

These general obligations reinforce shared responsibility across all levels of the Site and strengthen the effectiveness of the prevention system against money laundering and terrorist financing risks.

10.2. Functions and Responsibilities in AML/CFT Risk Prevention and Management

The prevention and management of money laundering and terrorist financing risks constitute an institutional responsibility involving all areas of the organization. Each area performs specific functions in accordance with its authority and role within the Site.

Senior Management is responsible for approving the general policies of the AML/CFT system (SPLAFT) and establishing the strategic guidelines that direct the Site's actions in prevention matters. Its responsibility includes defining corporate policies and allocating the resources necessary for the implementation of programs and internal controls.

Management performs an operational and supervisory role, ensuring the proper implementation of approved policies and coordination among the different areas of the Site. Its responsibility focuses on ensuring that procedures are applied consistently and that both business and support units integrate preventive measures into their daily activities.

The Compliance Officer performs a technical and specialized function, responsible for designing, updating, and overseeing the AML/CFT system (SPLAFT). Key responsibilities include the development of manuals and procedures, coordination of training programs, receipt and analysis of suspicious transaction reports, and communication with competent authorities.

Employees within operational and support units are responsible for applying established policies and procedures in their daily work, in accordance with the manual and the Code of Conduct. Their role focuses on the detection of unusual transactions, the timely reporting of suspicious activities, and the preservation of documentary traceability in each process.

In this way, the Site structures a prevention system in which functions and responsibilities are distributed in alignment with the authority of each level, consolidating a comprehensive AML/CFT risk management model.

10.3. Organizational Structure

The organizational structure ensures effective management of the AML/CFT system (SPLAFT), clearly defining the roles and responsibilities of each area involved in the prevention of money laundering and terrorist financing.

- Senior Management: Approves policies and allocates the necessary resources for system implementation. It is also responsible for approving the manual and ensuring the availability of resources for its execution.
- Compliance and Monitoring Manager: Oversees the operational implementation of policies, coordinates with different areas, and reports relevant incidents to Senior Management.
- Compliance Officer: Responsible for leading the implementation and management of the AML/CFT system (SPLAFT), preparing the manual, coordinating with relevant areas, and overseeing controls and reporting related to AML/CFT prevention. Additionally, acts as the formal liaison between the obligated entity, the supervisory authority, and the Financial Intelligence Unit (FIU).
- Compliance Specialist: Participates in drafting and structuring procedures, ensuring regulatory alignment and document consistency. Plays a key role in regulatory defense and the preparation of operational protocols.

- **Compliance Analyst:** Assists in information gathering, documentation of evidence, and preparation of risk matrices. Also supports the investigation of unusual or suspicious transactions, analyzes user profiles and transactional behavior, and contributes to maintaining updated records and controls within the AML/CFT system.
- **Monitoring and Fraud Unit:** Oversees daily transactions, identifies red flags, and generates periodic reports on potential money laundering or terrorist financing activities. Works closely with the Compliance Officer and Compliance Specialist to ensure timely responses.
- **Human Resources Department:** Ensures that key personnel are properly trained and committed to prevention policies. It also reinforces confidentiality in handling sensitive information and evaluates staff performance in relation to regulatory compliance.

XI. AML/CFT Risk Management Mechanisms

The Site adopts general management mechanisms aimed at identifying, assessing, and mitigating money laundering and terrorist financing risks. These mechanisms are structured around internal policies, control procedures, and analytical methodologies that allow operations, users, and suppliers to be classified according to risk exposure levels, applying proportional and traceable measures in each case.

11.1. Description of ML/TF Risk Factors

The Site's exposure to money laundering and terrorist financing risks is determined by various factors that directly impact its operations. These factors include both internal and external elements and must be assessed comprehensively to determine the level of institutional vulnerability and to implement appropriate preventive measures.

From an internal perspective, the organizational structure, the performance of the Board of Directors and management, employees' compliance with the Code of Conduct, the training received, and the robustness of internal processes are factors that may increase risk if not properly managed. Lack of supervision, high staff turnover in critical areas, or absence of documentary traceability are examples of situations that may weaken the prevention system.

From an external perspective, risk factors relate to the characteristics of users and suppliers, the nature of products and services offered, the distribution channels used, and the geographic jurisdictions involved in operations. Exposure increases when dealing with segments with unclear backgrounds, highly complex products, channels that hinder traceability, or countries with deficiencies in their prevention systems.

Finally, organizational culture is recognized as a cross-cutting factor influencing the effectiveness of the AML/CFT system (SPLAFT), as the level of ethical commitment and integration of prevention into corporate strategy determine the Site's ability to detect unusual transactions and take timely action.

11.2. Role of the Compliance Officer in Evaluating New Products and Markets

The Compliance Officer actively participates in evaluating proposals related to the launch of new products, entry into new markets, and any initiative that may involve exposure to ML/TF risks. This involvement takes place through structured stages that ensure the incorporation of regulatory and preventive criteria into strategic decision-making.

Initially, the Compliance Officer reviews proposals submitted by business units, identifying risk factors associated with the product, service, or market in question. This analysis considers the nature of operations, potential customer segments, distribution channels, and involved jurisdictions.

Subsequently, the Compliance Officer prepares a technical report documenting key observations and recommendations based on the analysis, which is submitted to Senior Management for review and consideration as part of internal evaluation and approval processes.

During the implementation phase, the Compliance Officer ensures that appropriate controls are incorporated into operational procedures, applying AML/CFT policies proportionally to the identified risk level. The officer also contributes to defining monitoring indicators and training personnel involved in the new product or market.

Finally, the Compliance Officer maintains continuous oversight, evaluating the effectiveness of implemented controls and proposing adjustments when new typologies, regulatory changes, or risk profile variations are identified.

11.3. Methodology and Criteria for Customer, Supplier, and Counterparty Due Diligence

The methodology applied for customer and supplier due diligence is a central component of the AML/CFT system. It includes identification and document verification procedures, economic and transactional profile analysis, as well as validation of the source of funds and legitimacy of operations. These criteria enable differentiated risk classification and the application of proportional due diligence measures, ensuring that business relationships remain transparent and traceable.

For suppliers, the evaluation focuses on confirming legal existence, reviewing background information, and verifying the jurisdiction in which they operate to identify potential vulnerabilities.

Regarding markets, correspondent banking relationships, money transfer companies, and other counterparties, the organization applies a general review approach aimed at assessing the regulatory environment and institutional reputation.

11.4. Background Screening of Employees and Management

The AML/CFT system includes procedures for evaluating the personal, professional, and financial background of employees, managers, and directors. This process aims to verify the suitability of individuals within the organization and ensure alignment with ethical and regulatory standards.

The assessment includes identity verification, general background checks, and potential links to risk-related activities. Professional experience and roles related to management and control are also considered, along with consistency between declared income and available records to identify potential red flags.

These procedures are carried out by the Human Resources and Compliance departments under the supervision of the Board of Directors. The Compliance Officer validates results and provides technical recommendations, while the Board ensures corrective actions where necessary.

This system supports preventive control over the integrity of key personnel and strengthens institutional trust and the effectiveness of the AML/CFT model.

11.5. Procedures for the Analysis of Alerts, Unusual Transactions, and Suspicious Activities

The AML/CFT system establishes a specific procedure for analyzing alerts, unusual transactions, and suspicious activities, ensuring traceability and proportionality in risk management.

In the initial phase, operational areas detect alerts generated by monitoring systems or internal reports, which are then submitted to the Compliance area for review. A detailed analysis follows, including verification of available information, evaluation of the user or supplier profile, and comparison with established behavioral patterns.

If an operation is classified as unusual, observations are documented and follow-up measures are applied to determine whether there is a legitimate explanation or persistent risk indicators. If classified as suspicious, the Compliance Officer prepares a technical report and submits it to the competent authorities in accordance with applicable regulations.

This process is supported by a feedback mechanism that allows for adjustments to monitoring parameters, strengthening of internal controls, and staff training in identifying red flags.

XII. Recordkeeping and Communication Procedures

Recordkeeping and communication procedures define how the organization documents relevant information and transmits internal and external reports related to AML/CFT risk prevention, ensuring traceability and regulatory compliance.

The Site establishes procedures for the registration, filing, and retention of AML/CFT-related information, including user transactions, identified alerts, internal analyses, and system reports.

Records are maintained using structured criteria of organization, integrity, and accessibility, in both physical and digital formats.

12.1. Internal Communication Channels

The Site recognizes the importance of having internal communication channels that enable coordination among the different areas of the organization, with the purpose of ensuring the effectiveness of the anti-money laundering and counter-terrorism financing

prevention system. These channels constitute an institutional mechanism that facilitates the transmission of relevant information, the discussion of findings, and the traceability of decisions made in compliance matters.

Communication is conducted in a formal and structured manner through reports, follow-up meetings, and the use of electronic means enabled by the organization. The Compliance Officer acts as the main liaison in this process, consolidating the information received.

12.2 Consultation Mechanisms between the Compliance Officer and Company Departments

The Site recognizes the importance of having consultation mechanisms that enable interaction between the Compliance Officer and the various departments of the organization, with the purpose of ensuring the effectiveness of the anti-money laundering and counter-terrorism financing prevention system. These mechanisms constitute an institutional framework that facilitates the exchange of information and the coordination of actions related to risk management.

Consultation is carried out through the communication channels available within the Site, allowing operational and administrative areas to provide relevant information to the Compliance Officer and receive guidance on the application of internal policies and applicable regulations.

XIII. International References and Regulatory Framework for AML/CFT Prevention

The Site recognizes and adopts as its reference framework the main international standards and regulations on the prevention of money laundering and terrorist financing. Among these, particular emphasis is placed on the recommendations of the Financial Action Task Force (FATF) and the provisions of the United Nations (UN).

These international guidelines complement the applicable national regulations and serve as the basis for the design of internal policies, procedures, and controls, ensuring that the AML/CFT system (SPLAFT) remains aligned with global best practices and regulatory requirements in each jurisdiction.

XIV. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) shall be applied to customers classified as high risk, such as Politically Exposed Persons (PEPs) or those originating from high-risk jurisdictions. PEPs shall be subject to additional scrutiny and more rigorous due diligence measures to mitigate associated risks.

XV. Evaluación basada en riesgos

- **Region One: Low Risk**

Customers located in low-risk regions or engaged in low-risk activities will be subject to regular monitoring but will not require intensive additional controls.

- **Region Two: Medium Risk**

Customers classified as medium risk, in accordance with the FIU-Peru classification, will be subject to enhanced monitoring and intermediate controls to ensure compliance.

- **Region Three: High Risk**

Customers considered high risk, particularly those from regions with high exposure to financial crimes, will be subject to intensive monitoring and Enhanced Due Diligence (EDD).

- **Enterprise-Wide Risk Assessment**

A comprehensive risk assessment will be conducted at the organizational level to ensure that all operations comply with AML/CFT regulations.

- **Money Laundering Risk Assessment**

Each customer will be individually assessed to determine their risk level, based on their transactional profile, source of funds, and other relevant characteristics.

XVI. Ongoing Monitoring

Continuous monitoring mechanisms shall be implemented for all transactions carried out on the platform, in order to identify patterns of alerts or unusual behavior. The process for reporting suspicious activities includes:

- Risk management practices
- Identification and verification procedures
- Identification and reporting of suspicious transactions
- Recordkeeping requirements

- Definition of significant and critical activities for detection purposes
- Identification of specific incidents that may trigger a reassessment of the risk-based approach

MIC Group Entertainment N.V. consistently implements monitoring processes, particularly when introducing new or potential future products and/or services offered to its customers. The Company also conducts evaluations that are implemented and adjusted as necessary to mitigate any potential risks of money laundering or terrorist financing, especially where new products or services may present vulnerabilities.

These measures include, but are not limited to:

- General transaction analysis over specific periods
- General analysis of new services/products used by customers, or the application of limits on activities related to such products or services