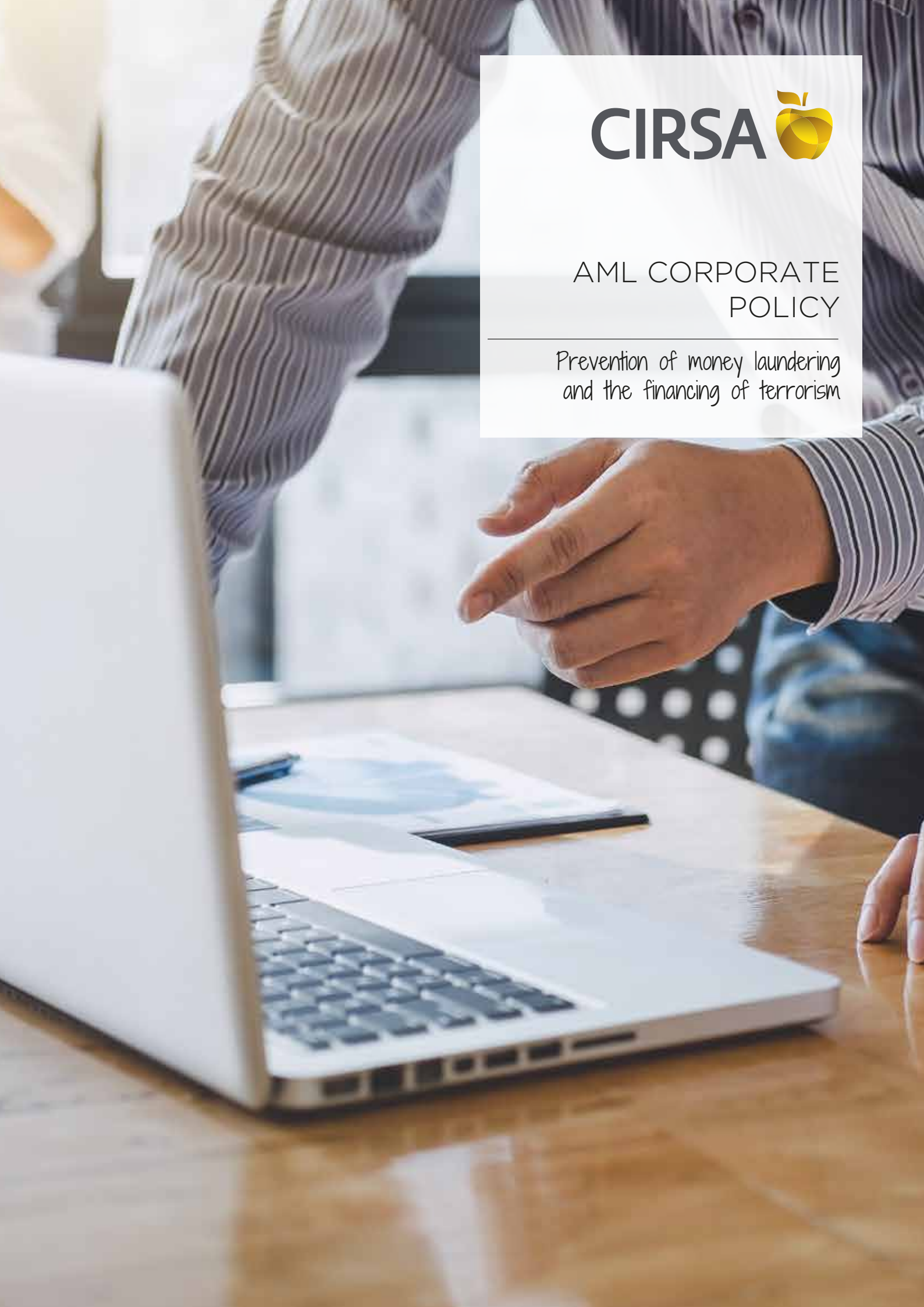

CIRSA

AML CORPORATE POLICY

Prevention of money laundering and the financing of terrorism

INDEX

1. INTRODUCTION

CIRSA Group is aware of the importance that large multinational companies play in the prevention of money laundering or in the laundering of assets and the financing of terrorism (hereinafter referred to as PML/FT) and as such expresses its total commitment to comply with the laws, regulations and recommendations made by international institutions that have been published with regard to this matter. The CIRSA Group applies resources and efforts in the fight against all forms of money laundering and the financing of terrorism.

With respect to this issue, the corporate policy of the CIRSA Group aims to ensure the efficacy of its model for the prevention of money laundering, which comprises the following elements:

- An organizational structure that possesses those resources necessary to manage and plan prevention functions, and which involves a clear assignment of those responsibilities attributable to each control body or unit.

- A regulatory body that determines those preventive measures and obligations required; with those related to client knowledge allocated given significant importance.

- The implementation of measures for providing information and the monitoring of client gaming operations in order to identify suspicious activities and to ensure that information is provided to the appropriate authorities.

- The implementation of communications and training plans for employees in order to maintain an adequate level of information and sensitivity, by providing those skills necessary for compliance with the applicable regulations.

- The continued communication between the head office and all CIRSA Group subsidiaries in all those countries in which the group is active, in order to guarantee effective monitoring and supervision activities.

- Finally, the need for an independent review in order to be able to verify and check the application and effectiveness of the remaining elements of the model in an independent manner.

1.1 Area of Application

This document establishes the minimum standards that group companies are required to meet, and it is applicable to all those companies and establishments that form part of the CIRSA Group that are reporting parties in the prevention of money laundering and the financing of terrorism, as well as all company administrators, managers and employees, regardless of the geographical location in which they perform their professional activities, notwithstanding their respect for and duty to comply with those laws and regulations applied in each country.

The application of the measures detailed in this policy must therefore guarantee due compliance with the applicable regulations in all those jurisdictional areas where the CIRSA Group is present and active in the gaming sector.

1.2 Approval

This policy has been approved by the Board of Directors of the main or parent company of the CIRSA Group in Spain; CIRSA ENTERPRISES, S.L.U. It has also been communicated to the administrative bodies of CIRSA Group companies in all those countries where they are active in order to ensure that they both take this policy into account and comply with it.

1.3 Money Laundering and the Financing of Terrorism

• **Money Laundering** is considered to involve:

- The conversion, the transfer of assets or monetary transactions in gaming operations in those establishments that belong to the CIRSA Group, and which is undertaken by parties who are aware that the aforementioned assets, capital or money have been derived from criminal activity in order to conceal or hide the illicit origin of the former financial assets, or in order to aid people who may be involved in such operations to avoid the legal consequences of their actions.

- The concealment or hiding of the nature, origin, location, disposition, movement or real ownership of assets or the rights over assets, undertaken by parties involved that are aware that said assets are derived from a criminal activity or from participation in a criminal activity.

- Participation in any of the activities mentioned in the above sections, association in order to undertake such acts, attempts to perpetrate them and the actions that involve helping, instigating or advising another party to carry them out or to facilitate their implementation.

• **The Financing of Terrorism,** the deposit, collection, use and delivery of goods, capital or money, by any means, be it directly or indirectly, with the intention of using these financial assets (or while being aware that they will be used) either wholly or partially, for the undertaking of the crimes of terrorism, as established in the penal

2. CORPORATE REGULATIONS

2.1 The Worldwide Application of the Corporate Policy

This Corporate Policy establishes the guidelines and the basic principles of the CIRSA Group's global prevention model in this matter, and all that which is not regulated in this policy must be supported by the laws, regulations and all other applicable rules that are applied in Spain and in other countries.

Furthermore, each of those CIRSA Group divisions or companies that are reporting parties, as defined in accordance with the provisions of Law 10/2010 on the Prevention of Money Laundering and the Financing of Terrorism in Spain, and by those laws applicable in each country where these bodies are active, will possess their own Manual on Procedures for the Prevention of Money Laundering and the Financing of Terrorism, which will establish the policies, procedures and internal control procedures that aim to ensure compliance with corporate policy and current legislation, in accordance with that inspired by the principles of this corporate policy.

2.2 Manuals and Regulations for Reporting Parties

The manuals of group organisations must be duly validated by the internal body for corporate monitoring and by its own respective administrative bodies, so guaranteeing that the company:

- Possesses adequate monitoring measures and internal control and communication bodies that approve appropriate policies and procedures in writing. The procedures and policies will concern due diligence, information, the preservation of documents, internal monitoring, evaluation and risk management, guarantees of compliance and communication. This will be implemented in order to prevent and impede the undertaking of operations related to money laundering and the financing of terrorism.

- Identifies and is informed about its clients, and that specific risk-based, client-acceptance policies are implemented and that it applies due diligence in the acceptance, identification and information processes applied to clients.

- Possesses staff who are responsible for compliance with the established provisions that seek to prevent money laundering.

- Complies with the requisites established in those laws that concern the acquisition and storing of client identification documents, and the registration and communication of operations.

- Creates and implements appropriate monitoring methods, based on the characteristics of each client and the corresponding operations performed, in order to detect the activities of any client who may be suspect, while immediately examining those operations detected and adopting those measures appropriate.

- Establishes an internal procedure so that its employees or managers may anonymously report legal infractions that have been committed within the reporting party.

- Bases its internal control procedures on a prior risk analysis, which is included in the Risk Self-Assessment Report and which is periodically reviewed.

- Performs and documents a specific risk analysis procedure prior to the launch of a new product, the provision of a new service or a new distribution channel, or the use of new technology, and appropriate measures are obligatorily applied to manage the risk.

- Performs a risk analysis of the client's characteristics. These will be classified into risk levels in order to design and implement measures and monitoring procedures to mitigate risk.

- Expressly communicates any actions or operations with the following characteristics to those internal bodies created for this purpose,: (i) that there are indications or the certainty exists that the actions observed are related to money laundering and the financing of terrorism or (ii) that the actions reveal an obvious lack of correspondence with the nature, volume of activity or operational history of the client in question, provided that in the previous analysis of the client's operations no economic, professional or business justification for the performance of these operations has been observed.

- Refrains from the execution of suspicious operations. When abstention is not possible or may hinder investigations, these operations may be performed, while immediately filing a report that details the reasons for the execution of the contract, in addition to noting those sections relevant to the communication of suspicious operations.

- Cooperates with financial intelligence units or other authorities, providing the information they require in the performance of their duties. This information may concern any data or information obtained by the reporting parties on the operations they perform and those persons involved in them.

- Undertakes training programmes on the prevention of money laundering and the financing of terrorism.

- Implements audit systems with respect to its policies and procedures for the prevention of money laundering.

- Establishes the duty of confidentiality in such a manner that both the corresponding entity and its managers and employees, who possess information about those operations or activities that are classified as suspicious are totally prohibited from disclosing to the client and to third parties the actions they are undertaking, although this prohibition does not include those bodies established for the internal prevention of money laundering. Any exception to this duty of confidentiality will be processed, in any of the cases applicable in law by the internal organisation appropriate.

3. ORGANISATION AND CORPORATE MONITORING

3.1 The Corporate Representative

Cirsa Group is represented on the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Infractions of the Bank of Spain by a corporate representative who is appointed by the Board of Directors of the CIRSA Group, and who is tasked with the functions assigned to him under Law 10/2010, as approved in Spain.

3.2 The Corporate Internal Control Committee

The Corporate Internal Control Committee (or OCI in its Spanish acronym) exercises its functions at group level and comprises members for each of the CIRSA Group divisions and corporate areas with management responsibilities in each of them.

Its function is to verify the effectiveness of the corporate policy on money laundering and the financing of terrorism; notwithstanding the effective implementation of an internal monitoring system with a primary level that is linked to the business divisions themselves, by reinforcing regulatory information in the most sensitive areas.

The OCI will hold several meetings each year, with the participation of the corporate representative, who will act as a secretary, and who will convene the meeting. Each year one of the members of the body will act as president, in accordance with an enumerated series of turns.

The OCI will be able to appoint Money Laundering Prevention Officers for specific activities, divisions or companies that manage operations that are considered to be of greater risk with respect to money laundering.

The functions of the OCI are those established in the regulations applicable in Spain, these regulations are adapted to the jurisdictional regulations of each country.

3.3 The Operational Technical Unit

The group also possesses a Corporate Operational Technical Unit (UPBC in its Spanish acronym) that is part of the Corporate Compliance Department. This body is tasked with coordinating all policies and actions in this area, and it also centralizes all CIRSA Group AML/FT activities.

Group entities will apply internal control measures, in accordance with this corporate policy and the criteria established by the OCI and by the UPC. Appropriate procedures regarding due diligence, information, document preservation, internal control, evaluation and risk management, in addition to guarantees of compliance and communication will be approved in writing.

The UPBC may appoint technicians to perform analyses in those companies and establishments that, due to a higher risk or business volume, require greater attention and vigilance.

The UPBC will inform the OCI on the evaluation of the effectiveness of the prevention measures implemented in the group.

4. MAIN OPERATIONAL ASPECTS

4.1 Due Diligence KYC

Client admission policy establishes a compliance framework at group level that may vary, depending on the risk level of the different gaming activities undertaken in each country and the type of clients.

The admissions policy must comply with international standards and the “Know Your Client” (KYC) principle, with a special focus on ensuring that good knowledge of the client and his activities is possessed at all times.

4.2 Detection, Monitoring and Operational Analysis

CIRSA Group companies must possess the means for the detection, monitoring and examination of operations. These means will be applied, depending on the risks and in all events they will comprise the basic aspects required for the detection of suspicious operations:

a. Internal communications by means of notifications from group employees.

b. The detection of potentially suspicious operations by means of the established alert systems (at the level of each group company and/or centralized systems).

c. The detection of suspicious operations will result in a detailed and comprehensive analysis that seeks to determine the effective existence of evidence of money laundering or the financing of terrorism.

d. Group companies will communicate on their own initiative to the supervisory and/or financial intelligence agencies any fact or operation, including mere attempts that once the special examination has concluded determine that the operation either possibly or verifiably involves connections to money laundering or the financing of terrorism. The supervisory bodies will be notified of operations that reveal an obvious lack of correspondence with the nature, volume of activity or operational history of the clients.

e. Group employees must refrain from undertaking any operations in which there may be some indication or certainty that these operations are linked to money laundering or the financing of terrorism.

f. Group employees, managers or agents must not disclose to the client or to third parties the fact that information has been communicated to the internal monitoring bodies, or the supervisory body, or that any operation is being examined or may be examined with respect to its potential links to money laundering or the financing of terrorism.

4.3 The Monitoring of the Sanctioned Clients List

Group companies and their establishments must verify if their clients are on the sanctioned client lists that are periodically published by the sanctioning agencies of the United Nations, the European Union or OFAC and on the local lists of each country, where such registration may be obligatory in the jurisdictional areas in which group companies carry out their activities.

They will also implement procedures in order to verify the access of persons with public responsibilities to their establishments, for the application of reinforced diligence measures, in accordance with the applicable regulations of each country.

5. CORPORATE TRAINING

Training and awareness training regarding the risks associated with these crimes is a key factor in the fight against money laundering and terrorism.

CIRSA Group companies undertake training programmes for their employees in order to guarantee an appropriate level of awareness among all staff, as required by law and they establish policies that guarantee mandatory prevention training for money laundering and the financing of terrorism (including senior management and administrative bodies) both periodically and as appropriate to the risk exposure levels of their activities.

The PML training programmes of all CIRSA Group companies must be validated by the UTOC, and records and evidence of the training courses held must be kept, in addition to their contents, and the details of those employees who have received and passed the training courses.

6. ENTRY INTO FORCE AND INTERPRETATION

This policy and any of its subsequent modifications and updates must be approved by the Board of Directors of the CIRSA Group on the proposal of the corporate control body.

The supervision of the correct adaptation of its content to group companies will be the responsibility of the Corporate Operational Technical Unit.

It will come into force on publication through internal communication channels and it will be periodically updated.

www.cirsa.com

2020

Ctra. de Castellar, 298 · 08226 Terrassa. Barcelona. Spain · T 34 93 728 33 18 · info@cirsa.com · www.cirsa.com