Corporate Policy on Crime Prevention, Anti-Fraud, Anti-bribery and Corruption

Version	Approved by:	Date:
v.1	Board of Directors CODERE S.A	27/02/2017
v.2	Board of Directors CODERE GROUP TOPCO	03/17/2025

1. Introduction

According to the Shareholder's Agreement related to Codere Group Topco (Schedule 1, Part A, Conduct of Business), the Company and the Group Companies shall comply with all Laws applicable to it in respect of the conduct of its business and in particular

- Comply with all Anti-Corruption Laws and Money Laundering Laws and maintain and enforce policies and procedures designed to prevent violations of Anti-Corruption Laws and Money Laundering Laws.

- maintain complete and accurate books and records, including records of payments to any Government Official or Government Entity in accordance with Anti-Corruption Laws, Money Laundering Laws and generally accepted accounting principles.

- not permit any Government Official to serve in any capacity within any Group Company, including as a director, employee, officer or consultant.

- adopt and implement proper and appropriate policies, procedures and measures designed to ensure that no Group Company nor any of its Agents from time to time is included on a Sanctions List, engaged in any dealings or transactions with any person on a Sanctions List or acts in a manner that is otherwise in violation of any Sanctions.

The Board of Directors of Codere Group Topco S.A. (the "**Company**") has the power to design, assess and continuously revise the Governance System, and specifically the guidelines governing the conduct of the Company and of the companies belonging to the Codere Group (the "**Group**").

This **Crime Prevention, Anti-fraud, Anti-bribery and Corruption Policy** responds to the desire of the Board of Directors of the Company to align the Group with the best practices of Corporate Governance in relation to the development of a compliance system on the regulations of the crimes, applying the standards established in the ISO 19600 standards on Compliance Management Systems and UNE 19601 on Criminal Compliance Management Systems.

Furthermore, it is aligned with the culture of integrity and respect for the rules of the Codere Group and takes into consideration not only the interests and strategic objectives of the Organisation but also the demands that may come from its Stakeholders and, consequently, with its determination not to tolerate any conduct that may constitute a criminal offence.

On the basis of this commitment to compliance, the parameters of conduct expected of the Subjects affected by this document are set out, requiring them to commit to them, describing the measures taken to monitor this mandate and the consequences in the event of noncompliance.

2. Regulatory Framework

This Policy shall always be governed by the pertinent legislation in force and any legislation amending or replacing it in the future, applying the concepts used by judges and Courts, taking into consideration the criteria on the Criminal Liability of Legal Entities.

In this context, it is essential to review the current systems for control, regulatory compliance and crime prevention, under the **Corporate Governance Framework** on Compliance, to ensure that the organisation and management model includes the following main principles: (i) the existence of Bodies with autonomous faculties, holding initiative and control, to supervise the operation and compliance with said prevention model; (ii) the identification of the company's activities in whose field crimes that should be prevented may be committed (risk map); (iii) the implementation of protocols or procedures that specify the shaping process of the will of the legal person to take decisions and put them into.

Finally, the necessary standards, guides or procedures for correct implementation, execution and compliance with this Policy shall be implemented at each Group company. The Governing Bodies of these companies will make the decisions necessary to integrate the provisions of this Policy.

3. Purpose

The objectives of these Policy are, principally:

(i) To convey to all employees, executives and members of the Governing Bodies of Codere the commitment of the entities to ensure that their activity is based on respect for the laws and regulations in force at all times, as well as in the promotion and defence of their corporate values and principles of action established in their Code of Ethics and, consequently, linked to their ethical values, ratifying their firm will to maintain a strictly compliant conduct in criminal matters.

(ii) To establish a general framework for the entity's Criminal Prevention Model, adapting it to the new regulatory provisions. The Model comprises the set of measures aimed at preventing, detecting and reacting to criminal behaviour and identifies the risks and controls associated with the same that are established.

(iii) To assure shareholders, customers, suppliers, judicial bodies and society in general that the Codere Group complies with its duties of supervision and control of its activity, establishing appropriate measures to prevent or reduce the risk of crimes being committed and that, therefore, the legally appropriate control is exercised over directors, executives, employees and other associated persons.

(iv) In addition, Codere Group has defined the different criminal offences which, in accordance with the legal provisions applicable, may be imputable to legal entities, distinguishing, firstly, those offences whose potential risk of commission, based on the corporate purpose and ordinary activity carried out by Codere Group, and the other entities that make up the Perimeter, could be higher and, secondly, the other behaviours that may have criminal relevance as they are associated in the legislation with a possible commission by legal persons.

4. Scope of Application

This Policy applies to employees, executives of the Codere Group and the directors and board members of Company and the Group Companies. Adherence to this Policy by the Governing

Bodies of subsidiaries shall be made to supervise and coordinate the criminal prevention model implementation in those subsidiaries and shall undergo a minimum annual review to determine whether the relevant requirements are met.

In any event, Codere's compliance function, given its corporate nature, shall ensure the integration of this Policy in the subsidiaries.

This Policy is applicable to all activities and business carried out by Codere.

In addition to this Policy, there is a **Catalogue of Criminal Risks**, which summarises the different criminal offences for which legal persons may incur criminal liability. These criminal offences are for offences committed in the name or on behalf of, and for their direct or indirect benefit, (i) by their legal representatives and de jure or de facto directors, or (ii) by persons under their authority, when the commission of the offence, in the latter case, is the result of a lack of due control, given the specific circumstances of the case.

For each of the offences described, the main activities that could entail Criminal Risks are listed for the purpose of alerting members of Codere and its Business Partners to situations that could expose them to such criminal risks in the exercise of their activities. Thus, if you have any doubts regarding the content of the Catalogue or wish to obtain further information, please contact **compliance@codere.com**

5. General principles

The principles that govern this Policy are as follows:

1. Act in accordance with current legislation, the Code of Conduct and Ethics, and other internal rules and standards.
2. Promote a corporate culture of crime prevention and refusal to tolerate unlawful or fraudulent acts, while promoting ethical principles and responsible behaviour.
3. Always guarantee the existence of efficient, permanent, and up-to-date control systems.
4. Ensure that all activities and all decisions made by Codere and Perimeter companies are made subject to the internal rules, procedures, protocols, and controls in place for that purpose. In the event of Related Parties, these activities and decisions will be those set out in the contract governing the service in question.
5. Ensure the appropriate resources and means for the application of these General Principles to prevent or detect criminal offences possibly being committed.
6. Carry out training activities that are suitable and provided often enough to ensure knowledge in this matter remains up-to-date and the development of a culture of business ethics and legal compliance.
7. Transmit the accountability of all physical and legal persons under the scope of application of these General Principles regarding monitoring potentially illegal behaviour in criminal terms. Specifically, those who oversee employees or teams shall ensure that they prevent unlawful criminal behaviour and report as soon as possible and in due fashion to the established bodies and implement processes as soon as they detect any such behaviour.
8. Transmit the obligation of all persons subject to these General Principles to report any circumstance or event that comes to light and that might constitute a crime or fraudulent or irregular situation.
9. Foster a culture of compliance to help ensure that criminal risks and non-compliances are duly reported through the internal channels set up for this purpose to the body responsible for safeguarding the operation of and compliance with the prevention model, while also ensuring the anonymity of the whistle-blower.
10. Investigate, as soon as possible, any events or situations presumed to be criminal, while protecting the rights of the people investigated and the whistle- blower.
11. Ensure awareness of the disciplinary procedures and sanctions in place to respond to internal noncompliances that might constitute criminal offences in accordance with internal regulations and applicable law in accordance with the provisions of the Collective Bargaining Agreement and the Workers' Statute and other applicable legislation.

6. Crime Prevention Model

In this context, it is essential to ensure that there is an organisational and management model in place for the prevention of crime, including the appropriate control and regulatory compliance systems to help ensure that the companies do not incur any such liability.

The main aspects of the Model are:

1. The specific naming of all activities at Codere and Perimeter companies that could lead to the perpetration of criminal offences that should and must be prevented.

2. Implementation of organisational measures and procedures to steer the process of forming opinions, making decisions and acting on those decisions at the legal person.

3. Appropriate resources to stop crimes that should be prevented from being committed.

4. The obligation to report possible risks and non-compliances to the body responsible for monitoring the proper functioning of the prevention model and enforcing compliance.

5. Periodic verification of the model and its modification where appropriate or where changes occur in the organization, control structure or activity undertaken.

The Model features five (5) different phases:

1. **Prevention:** identification of possible criminal conduct that affects Codere and the companies within its Perimeter, while also determining the existence of related controls.
2. **Detection:** detection of possible criminal acts through different existing channels and methods.
3. **Response:** action in response to any evidence or suspicion of a crime being committed at Codere or any of the companies within its Perimeter and the reduction, insofar as possible, of any ensuing damage.
4. **Report:** periodic communication and information for Company governance and management bodies and, where applicable, at the companies within its Perimeter.
5. **Monitoring:** periodic assessment of the Model and tailoring it to the specific circumstances of Codere and the companies within its Perimeter, as well as possible changes and developments in crime prevention at legal persons in accordance with applicable legislation, case law and academic opinion. To carry out this periodic

assessment, the Model will undergo an audit at least once every three years, which may be internal or external.

7. Crime Prevention Programme

As regards the basic principle relating to the identification and evaluation of the risks relating to improper conduct and acts that are illegal or contrary to law or to the Governance System, Codere Group has implemented a specific and effective programme for the prevention of crimes (understood as a group of measures intended to prevent and mitigate the risk of commission of potential crimes and to detect and react to the commission thereof).

The purpose of such programme is: (i) to strengthen the existing commitment of the Company and of the other companies of the Group to combat the commission of crimes, particularly all forms of corruption and fraud; and (ii) to assure third parties and judicial and administrative authorities that the Company and the other companies of the Group effectively comply with the duties of supervision, monitoring and control of their activities by establishing appropriate measures to prevent crimes −or to significantly reduce the risk of the commission thereof− and that, therefore, said companies exercise due control over the members of their management bodies, their professionals, and other subordinates, based on their governance model, as is legally required thereof, including the monitoring of possible situations of crime risk that may arise within the scope of their activities, even in those cases in which such situations cannot be attributed to a specific individual.

The Crime Prevention Programme is made up of:

- The **general control environment** at the companies of the Codere Group.
- The **criminal risk registers** setting out the risks of commission of unlawful acts that affect the companies of the Group as well as the existing controls to minimise their exposure to them.
- The set of internal **regulations and provisions** based on their significance within this Programme.
- The **processes** implementing and putting into practice the provisions of the regulations, and which include controls to mitigate the risks identified, and which

are intended to ensure compliance with the internal regulations and policies.

- The **penalty system** established on a general basis, in the Corporate Policy on the Comprehensive Disciplinary Programme and in the corporate Regulation for the elaboration and organisation of the regulatory framework in order to ensure compliance by all employees with the regulations and procedures established at the companies of the Group.

- The existence of a **Crime Prevention Function** with responsibility for implementation, development, compliance and review as well as continuous improvement.

- The existence of a **reporting channel**, through which any employee must confidentially report any indication of the commission of a crime.

- **Training and information** regarding the compliance of the internal regulations, for all employees of the companies of the Group (including specific training about crime prevention, as set in this Policy)

At least once per year, the Company's Compliance Committe shall evaluate compliance with and the effectiveness of its crime prevention programme and shall assess whether regular modification and update thereof is appropriate, provided that the circumstances so require.

8. Roles and responsabilities

The roles and responsibilities must respect the need to achieve collaboration among the Group, Codere entities and the functions.
Above all, the responsibilities of the Board of Directors of the Company are the creation, maintenance and supervision of this general control environment.

Specific organisational units:

Compliance Unit is the unit responsible to supervise the operation, implementation, development, compliance with and communication of the Crime Prevention Programme.

To this end, its mission will be to identify the specific criminal risks, overseeing evaluating, analyzing, implementing, improving and monitoring the Crime Prevention.

The responsibilities attributed to it by the Policy are carried out in the following functions:

(i) Manage the Group's criminal risk through control methodologies and tools.
(ii) Establish and update the Group's risk map and criminal controls based on regulatory developments, the activity of the different Group companies and the relevant infractions that have occurred.
(iii) Assign responsibilities by identifying those responsible and executing the controls established to mitigate criminal risk.

Head of Compliance Fuction in each country carry our in the following functions:

(i) Document the controls carried out to verify compliance with established standards.
(ii) Evaluate, at least once a year, compliance and effectiveness of the Policy and programs for the prevention of the commission of crimes.

(iii) Manage in their areas the procedures, alerts and controls that prevent criminal risk, communicating situations that affect the effectiveness of said controls. To this end, they appoint those responsible for controls related to their areas.

Ethics, Crime Prevention and Antifraud Committee in each country, which, among other responsibilities, (i) manage and supervises the operation and compliance with the implemented crime prevention programme in each country and, (ii) know and follow up, the internal investigations about suspicious acts, situations or facts that could be opened in relation with that proofs and controls or, in general, with the application of the Programme.

Without prejudice to the existence of an Ethics, Crime Prevention, and Antifraud Committee in each country, the responsibilities above related to the scope of the Group's Holding Companies at the corporate level may be assumed by a country committee designated for this purpose. In such a case, the Group's Compliance Manager or their delegate, as well as a corporate representative from human resources and corporate auditing, will be part of the committee.

Codere Group Companies must have an appropriate organisational and governance structure to report in line with the requirements established in law and regulations based on their significance within the Programme.

The Group Companies Directors are responsible for preventing and detecting, in relation

to the assigned control, any allegedly criminal act or irregular act that is contrary to the applicable internal and external regulations. Those responsible for controls will have the functions:

(i) Ensure the correct execution of the controls in accordance with the corresponding control procedure, although they will not necessarily be the executors of the controls.
(ii) Collaborate in the prevention and detection of crimes in their respective areas, including the communication of operations suspected of constituting crimes.

Internal Audit Unit, which reports directly to the Board of Directors, through the Audit and Control Committee, and which, according to its functions and Task Plan and in an independent manner, supervises the internal control structures of the Group.

Other corporate units that control specific compliance risks relating to regulation, privacy, competition, environment, supply chain, commerce activity, tax, security and systems and employment-related risks.

9. Crime Prevention Function

The Crime Prevention Function shall be carried out by the Compliance Function (Compliance) who, in collaboration with the Internal Audit and the Legal Services, which shall perform duties relating to the design, documentation, update and monitoring of the Crime Prevention Programme.

The Crime Prevention Function has the following powers, among others:

a. To drive and coordinate the review, updating and improvement of the Crime Prevention Programme, which shall include the updating of the risk register. This review shall be performed based on a model that establishes a variable review frequency for each company based on the volume and risk thereof, as well as when the regulatory or jurisprudential changes so advise.

b. To define the objectives, scope and priorities of the model for assessing the Crime Prevention Programme and, where applicable, of the compliance management against crime system which may be in place as well as monitor the said objectives etc.

c. To propose required modifications or updates to the Crime Prevention Programme, and particularly improvements that should be applied in view of the conclusions reached during prior reviews and potential breaches detected through ongoing supervision of the Model.

d. To know with all the required detail and evaluate the results of the tests performed in the review of the Programme.

e. On a general basis, to promote and supervise the resolution of incidents, as well as the implementation and monitoring of recommendations to improve the Programme that may have been made, whether that be because of the verification mentioned in the following section or because of any other matter.

f. To regularly report to the Compliance Committee of the Company on the operation of the Programme, including material breaches or incidents detected, as well as on the plan of action or measures adopted to resolve them.

10. Registration of Criminal Risks: Identificationand Assessment of Risks

Codere and the various companies of its Group put into practice the provisions of the regulations, implementing a process of identifying the criminal risks that might affect the Group, creating a register of criminal risks.

The register of criminal risks is a written description, after a detailed analysis, of the potential criminal contingencies that might affect the various legal entities of the Codere Group, with an identification and specific assessment of the existing risk.

There has also been a particular identification of the controls existing at the various companies of the Codere Group that mitigate these risks, and the effectiveness of the said controls has been verified.

11. Audit of the programme's operation

The operation of the Crime Prevention Programme will be subject to an audit to be carried out with the periodicity necessary in response to the circumstances in each company, although this will be considered especially on:

(i) Changes in the organisation or control structure.
(ii) Changes in the activity carried out by the company that could eventually result in a necessary expansion of the scope of control.
(iii) Modifications in the Criminal Code or in its jurisprudential interpretation in areas that affect the activity of the company.
(iv) Any other objective circumstances that may substantially alter the risk profile of the Company and the Group companies.

12. Anti-fraud, Anti-bribery and Corruption

The term **fraud** is used to describe a whole range of activities such as: deception; **bribery**; forgery; extortion; **corruption;** theft; conspiracy; embezzlement; misappropriation; false representation/accounting, concealment of material facts and collusion and **money laundering**.

Generally, however, fraud involves the intention to deceive a person or organisation to obtain a financial advantage, or personal gain, or to cause a loss to another party.

The term fraud also includes the use of information technology equipment to manipulate programmes or data dishonestly.

Bribery involves an inducement or reward offered, promised, provided or received in order to gain or give any commercial, contractual regulatory or personal advantage.

Corruption is the misuse of entrusted power for personal gain. This would include dishonest or fraudulent behavior by those in positions of power, such as managers or government officials. It would include offering, giving and receiving bribes to influence the actions of someone in a position of power or influence, and the diversion of funds for private gain.

Money Laundering is attempts to make illegally obtained money appear legitimate.

Codere Group takes the most serious view of any attempt to commit fraud by employees, staff, suppliers, contractors, suppliers and others.

Fraud, Bribery and Money Laundering are criminal offences and qualify as acts of gross misconduct.

13. Principles of conduct and responsabilities

To manage the exposure to fraud, bribery and corruption, thia policy covers the key principles to be applied to ensure that Codere Group continue to have high standards and clear guidance on the organisational approach to addressing the risks of fraud, bribery and corruption and sets out our responsibilities for its prevention.

Principles of conduct

a. Not tolerate, permit or engage in any conduct constituting corruption in any of its forms, including extortion or bribery, in the course of business or professional activities or in relations with the public or private sector.

b. Promote a preventive culture based on the principle of “zero tolerance” for business corruption and bribery, as well as for the commission of other acts constituting any form of fraud.

   This “zero tolerance” principle for business corruption, bribery and any form of fraud is absolute in nature and takes precedence over the possibility of obtaining any type of benefit (financial or otherwise) for the Company and for the other companies of the Group, as well as for their directors, professionals and suppliers, when based on a business or transaction that is improper, illegal or contrary to law or to the Governance and Sustainability System, and particularly the ethical principles of the *Code of Ethics*.

c. Take appropriate measures so that relations between the professionals of the companies of the Group and any government administration, authorities, officials or other persons who participate in the exercise of public functions, as well as political parties and similar institutions, are any event governed by the principles of cooperation, transparency and honesty.

d. Have specific procedures to prevent any conduct that might be considered an act of corruption, the application of which must be supervised by the Company's Compliance Unit or by the compliance units of the companies of the Group, as applicable.

e. Implement appropriate training programmes and communication plans for the professionals of the Group with a frequency sufficient to ensure that their knowledge in the area covered by this Policy is kept up to date. In particular, the professionals of the companies of the Group shall receive specific training regarding the content of the Code of Ethics to prevent any instance of fraud and corruption in any form.

f. Identify and assess the risks associated with all forms of fraud and corruption in the activities of the Company and of the other companies of the Group.

g. Establish the appropriate controls and preventive measures (including, without limitation, through the internal rules and procedures approved for this purpose) for the identification, control, mitigation and prevention of all forms of fraud and corruption, and particularly in all activities involving third-party relationships.

h. Ensure that the relationship between the companies of the Group and their suppliers is based on legality, business ethics, efficiency, transparency and honesty and that no supplier of the Group's companies offers or gives to officials and other persons who participate in the exercise of public functions, authorities, third parties or any professional of the Group's companies, within the context of the business activity carried out for or on behalf of the Group, whether directly or indirectly, gifts, presents or other improper benefits or unauthorised advantages, whether in cash or otherwise, in order to secure favourable treatment in the award or maintenance of contracts or in business relations or to obtain benefits for themselves or for the supplier company.

i. Promote appropriate measures to ensure that suppliers comply with the policies, rules and procedures established within the Group's boundary in connection with the prevention of corruption in any of its forms.

j. Conflicts of interest must be identified and managed in accordance with the provisions set forth in the internal regulations on Conflict of Interest. In the event that an employee finds himself/herself in a situation of conflict of interest, or believes that it may be perceived as such, he/she must always report it to his/her direct manager and register it through the tools that the Codere Group makes available to him/her

The Company and other companies of the Group have activated appropriate channels so that the members of their management decision-making body, its professionals, its

suppliers and other third parties determined by applicable legal provisions can report potentially improper conduct or acts that are potentially illegal or contrary to law or to the Governance and Sustainability System that concern or affect the their respective activities, including, in particular, acts and conduct that are potentially fraudulent or facilitate corruption in any of its forms.

Likewise, specific principles for action must be followed and complied in relation to those activities and processes that involve a greater risk of corruption, such as, for example: the offer, delivery and acceptance of gifts or personal benefits; the invitation to or attendance at events: professional and travel expenses: donations and sponsorships; relationships with third parties (i.e. suppliers, agents, intermediaries and business partners); the selection and recruitment procedures or facilitation payments.

Responsibilities

Line managers are responsible for the prevention and detection of fraud by undertaking training at induction and refresher training aiming to ensure that an adequate system of internal controls exists within their areas of responsibility, and these controls operate effectively. This is to aim to ensure that all their employees are aware, trained, understand with the assurance that the policy is being complied with and complying with any regulatory requirements.

Every employee, staff, contractors and other third parties have a responsibility to adhere to this policy and should: alert their line manager or main most senior contact at the Codere Group where they believe the opportunity for fraud exists because of poor procedures or lack of effective supervision; report details of:

a. any suspected or actual fraud, or

b. any suspicious acts or events with their line manager, head of department.

Alternatively, employees can use the whistleblowing policy and assist in any investigations by making available all relevant information and by co-operating in interviews.

14. Key aspects on the prevention of bribery and corruption.

To promote compliance with the above general and specific principles for action, aside from its continuous monitoring and supervision, Codere Group:

- Account, records and documents all transactions, income and expenses in an appropriate and accurate manner, without omitting, hiding or altering data or information in relation to them; so that the accounting and operational records reflect the true image and can be verified by the supervisory departments and by internal and external auditors.
- It makes available to employees and third parties not belonging to Codere Group the Whistleblowing Channel where they can report indications or suspicions of corrupt practices within Codere Group or the existence of a risk of corruption or a breach of the Policy. Codere shall ensure the confidentiality and safety of complainants and shall not take, or permit, any reprisals or adverse consequences against those who, in good faith, make use of the Whistleblowing Channel in accordance with the provisions of the internal regulations on the management of Whistleblower Channel communications.
- Has in place a disciplinary system that can lead to termination of the employment or commercial relationships, as appropriate, and in accordance with the applicable laws and
- Ensures the objectivity and independence of Compliance, which has been entrusted with the task of promoting and supervising that Codere acts with integrity, particularly in the field of the prevention of corruption.
- All Codere Group members undergo specific training courses in this field, adapted to their professional activities.

15. Implementation of the Policy

The Compliance Fuction in each country proactively endeavours to ensure the application and effectiveness of this Policy and disseminates the content hereof among the people to whom it is addressed, all without prejudice to the responsibilities assigned to other bodies and divisions of the Company and, if appropriate, the administrative and management bodies of the country subholding companies and head of business companies and the respective compliance units of these companies.

16. Monitoring, Follow-up & Supervision

The Company's Compliance Unit shall be responsible for the continuous monitoring and followup of the provisions of this Policy.

It will also be responsible for promoting actions for its appropriate dissemination and knowledge.

The Internal Audit department shall review the adequacy and effectiveness of the measures applied, issuing the corresponding report to be submitted to the Audit Committee.

17. Approval, effective date and updating

This Policy shall enter into force on the date of its approval by the Board of Directors of the Company.

This Policy shall be kept up to date over time. To this end, it must be reviewed on a regular annual basis, and on an extraordinary basis, and in any case as soon as possible, when there are variations in the strategic objectives or an external or internal regulatory change that implies its updating or modification.

The Company`s Compliance Unit is responsible for assessing any proposal for modification.

18. Revision of the Policy

The Compliance Committee shall regularly review the contents of the Policy, ensuring that it reflects the recommendations and best international practices from time to time in effect, and shall propose to the Company's Board of Directors those amendments that contribute to the development and ongoing improvement thereof, taking into account any suggestions or proposals made by the Compliance Unit.

This Policy was approved by the Board of Directors on March 17, 2025.