Crime Prevention Model of Vemoris Group S.A.

APPROVED BY	DATE OF APPROVAL	VERSION
the Board of Directors of Vemoris Group S.A.	November 13, 2026	1.0

Introduction

This document summarizes the Crime Prevention Model of Vemoris Group (hereinafter, "the Model"): what it seeks to prevent, who is in charge, how it works and what is expected of each person. This is the public version: the detailed internal procedures are not part of it.

The Model develops section 10 of the Code of Ethics and is complemented by the Free Competition Policy.

1. Purpose and legal framework

1. The purpose of the Model is to prevent and detect crimes that may be committed in the course of the group's activities and that may give rise to criminal liability for the group's legal entities.
2. The Model is based on Law No. 20,393 on the criminal liability of legal entities, and on Law No. 21,595 on Economic Crimes, which expanded the crimes that can give rise to that liability and updated the requirements for prevention models.
3. Under the law, the Model must include, at a minimum:
   - the identification of the activities or processes that involve a risk of criminal conduct;
   - protocols and procedures to prevent and detect such conduct, including secure reporting channels and internal sanctions;
   - one or more persons responsible for applying them, with independence, effective powers and direct access to management;
   - periodic evaluations by independent third parties and mechanisms to improve and update it.

2. Scope

1. The Model applies to Vemoris Group S.A. and to its companies and business areas (hereinafter, "the group").
2. It is binding on directors, managers, employees, advisors and any person acting on behalf of or for the account of the group (hereinafter, "the group's people").

3. We expect suppliers, contractors and business partners to act according to equivalent standards. The group may include compliance clauses in the contracts it enters into with them.

3. Crimes it seeks to prevent

1. Law No. 20,393, as amended by Law No. 21,595, covers a broad catalog of crimes. Among the most relevant to the group's activities are:
   - money laundering and terrorist financing;
   - bribery of public officials, domestic or foreign;
   - private-sector corruption;
   - handling of stolen goods;
   - unfair management and misappropriation;
   - securities market crimes, such as the use of inside information;
   - tax crimes;
   - computer crimes (Law No. 21,459);
   - crimes against free competition (collusion, Decree Law No. 211);
   - environmental crimes.
2. This list is for guidance only. The Model covers all crimes that the law in force links to the criminal liability of legal entities.

4. Crime Prevention Officer

1. The Board of Directors appoints the group's General Manager as **Crime Prevention Officer** (hereinafter, "the Officer"). The Officer is responsible for applying the Model, on the terms required by law.
2. The Board of Directors ensures the Officer has sufficient autonomy, resources and powers to perform this role, and direct access to the Board to report on their work.
3. The Officer's main duties are:
   - identifying and updating the Model's risks and controls;
   - communicating the Model and organizing training;
   - receiving questions and reports, and investigating them or commissioning their investigation;
   - proposing improvements to the Model and sanctions to the Board of Directors where appropriate;
   - reporting to the Board of Directors, at least once a year, on how the Model is working.
4. If a question or report involves the Officer, it is handled by whomever the Board of Directors designates.

5. Risk activities

Vemoris Group is a holding company that invests its own capital and brings together companies from different sectors. Its main activities with a risk of criminal conduct are:

1. **Investments and divestments.** Buying and selling market instruments and interests in companies: risk of use of inside information, money laundering and transactions with counterparties of unknown origin.
2. **Movements of funds within the group.** Capital contributions, loans and transactions between group companies or with related parties: risk of unfair management, misappropriation and transactions that do not serve the company's interest.
3. **Relationships with banks, brokers and custodians.** Opening accounts, payment instructions and transfers: risk of money laundering and unauthorized payments.
4. **Hiring suppliers, advisors and intermediaries.** Risk of unsupported payments, non-existent services or a third party offering improper benefits on the group's behalf.
5. **Relationships with authorities and public officials.** Permits, inspections, tax and municipal procedures: risk of bribery.
6. **Donations, sponsorships, gifts and invitations.** Risk of their being used to obtain an improper benefit.
7. **Accounting and taxes.** Risk of false or incomplete records and of tax crimes.
8. **Systems and data.** Risk of unauthorized access, information leaks and computer crimes.
9. **New projects.** Launching new companies or products, including projects under development: risk of offering products or services to the public without first complying with the regulations that apply to them.

6. Controls

For each risk activity, the group applies controls such as the following:

1. **Counterparty due diligence.** Before investing, contracting or entering into a partnership, the counterparty's identity and reputation are verified and, where appropriate, the lawful origin of its funds.
2. **Approvals and segregation of duties.** Significant investments, payments and contracts require approval according to defined authorization levels, and whoever proposes a transaction is not the one who approves and pays it.
3. **Payments and accounts.** Every payment is made to accounts in the counterparty's name, against a supporting document and with an accounting record. No cash payments are made, except minor ones authorized by the internal procedure.
4. **Related-party transactions.** They are governed by Law No. 18,046 on Corporations and the bylaws, and are carried out on fair terms similar to those prevailing in the market.

5. **Inside information.** Confidential information is handled with restricted access. People who know it do not buy or sell the related securities, nor disclose it to third parties, in accordance with Law No. 18,045 on the Securities Market.
6. **Relationships with public officials.** Meetings with authorities are held transparently and in compliance with Law No. 20,730 on lobbying. No improper benefits are offered or given.
7. **Gifts, donations and sponsorships.** The rules of the Code of Ethics apply: only courtesies of symbolic value, and donations and sponsorships approved in advance, documented and with a legitimate recipient and purpose.
8. **Compliance clauses.** Contracts with suppliers, advisors and intermediaries may include the obligation to comply with the law and the Code of Ethics, and the group's right to terminate the contract if they do not.
9. **Accounting records.** Every transaction is recorded faithfully and on time. There are no off-the-books accounts or transactions.
10. **Information security.** Access credentials are personal and non-transferable, and access is granted according to each person's role.
11. **Legal review of new projects.** Every new product, service or company is legally reviewed before its market launch. The group does not raise or manage money from the public.

7. Whistleblower channel

1. Anyone, whether within the group or outside it, may report in good faith any facts that may constitute a crime or breach the Model through the **Whistleblower Channel** (**www.vemoris.cl/gobierno-corporativo/canal-de-denuncias**) or by writing to **contacto@vemoris.cl**.
2. Reports may be **named or anonymous**. The group safeguards the **confidentiality** of the whistleblower, of those involved and of the information.
3. **No retaliation.** The group does not tolerate retaliation against anyone who reports in good faith or cooperates in an investigation.
4. **Investigation.** The Officer investigates reports objectively and respecting the right of those involved to be heard, within 30 business days, which may be extended once, in accordance with section 12 of the Code of Ethics.
5. If the facts could constitute a crime, the group will assess with legal counsel whether to bring them to the attention of the competent authorities.

8. Training and communication

1. The Model and the Code of Ethics are made known to all of the group's people when they join and whenever they are amended.
2. The group provides periodic training on the Model, with content adapted to each person's role, especially for those involved in risk activities.
3. Attendance at training sessions is recorded.

9. Sanctions

1. Non-compliance with the Model may give rise to the measures provided for in the Internal Regulations, the contracts and the law, without prejudice to any civil or criminal actions that may apply.
2. Measures are applied respecting the person's right to be heard, and in proportion to the seriousness of the offense.
3. No one may ask another person to breach the Model, nor justify a breach on the grounds of an order from a superior.

10. Supervision and review

1. The Officer supervises how the Model works and how its controls are applied, and reports to the Board of Directors at least once a year.
2. The Model is reviewed at least once a year, and also whenever the law, the group's activities or its risks change, or when a control is found to have failed.
3. As required by law, the Model will be periodically evaluated by independent third parties, and their conclusions will be used to improve and update it.

11. Effective date

This Model is effective from its approval by the Board of Directors of Vemoris Group S.A. Any amendments will be communicated to all of the group's people.



Approved by the Board of Directors of Vemoris Group S.A. — November 13, 2026

This is an English translation of the original Spanish document. In case of any discrepancy, the Spanish version prevails.