

## **1. PURPOSE**

- 1.1. The Risk Management Policy ("Policy") aims to establish the principles, guidelines and responsibilities to be adopted by ENEVA S.A. ("ENEVA") in the process of risk management, so as to enable the identification, assessment, handling, monitoring and communication of Risks to the Administrators, allowing a lower level of uncertainty in the achievement of goals and the preservation of the value and perpetuity of the company's business. In addition, it aims to promote the integrated management of all risks to which ENEVA is exposed, including: financial, strategic, operational, regulatory risks, among others.

## **2. APPLICATION**

- 2.1. This Policy applies to ENEVA and its subsidiaries, as well as to its employees, Administrators and members of the Fiscal Council, if in operation.

## **3. DEFINITIONS**

**Risk appetite:** level of exposure to Risks that the Company is willing to accept in implementing its business strategies and performing its activities in order to achieve its goals.

**Administrators:** members of the Board of Directors and Company's Executive Officers.

**Employees:** all employees of the Company.

**Company:** means ENEVA S.A. and its subsidiaries.

**Lines of Defense:** concept that defines roles, responsibilities in managing Risks and strengthening governance, as well as the interaction of these roles at all Company's levels.

**Risks:** any threat of an event or action, external or internal, that may negatively affect the achievement of the Company's goals, businesses and business opportunities or its processes.

**Strategic Risk:** possibility of implementing an unsuccessful or ineffective strategy that fails to achieve the intended returns.

**Operational Risk:** possibility of incurring losses resulting from failure, deficiency or inadequacy of internal processes, people and technological environment, or external events. Includes the legal risk, associated with the inadequacy or deficiency in agreements entered into by the Company, as well as sanctions due to non-compliance with legal provisions and indemnities for damages to third parties resulting from the activities performed by the Company. Operational risk events include internal and external fraud; legal proceedings, poor workplace safety; inappropriate practices relating to customers, products and services; damage to physical assets; and those that may lead to interruption of the Company's activities and failures in information technology systems and infrastructure.

**Financial Risk:** means any risk associated with ENEVA's finance, including market, credit and liquidity risks, in financial transactions. It is commonly understood as the risk of potential financial loss and uncertainty about a business (acquisition, divestment, loans, among others).

**Regulatory Risk:** possibility of changes in regulations and actions by regulatory bodies, whether at the international or local level, which may result in increasing competitive pressure and significantly affect the Company's ability to efficiently manage its business.

#### **4. PRINCIPLES**

- 4.1. Risk management process shall comply with ENEVA's ethical principles, values and culture. Information generated by the Risk management system shall be reliable, in compliance with legal guidelines, and shall provide subsidies for decision-making aimed at adapting the level of exposure to Risks and prioritizing improvement actions.
- 4.2. Risk management shall support ENEVA's growth plan, strategic planning and business continuity, ensuring the preservation of cash flow and strengthening the company's capital structure and asset management.
- 4.3. Risk mitigation depends on the structured implementation of models, controls, systems, and protection mechanisms that shall not have a single form or model, and priority shall always be given to the one that best adapts to the process, structure and available resources.
- 4.4. Management bodies are responsible for disseminating the Risk management culture at ENEVA and for ensuring adequate resources for the implementation of the processes of

identification, assessment, handling, monitoring and communication of Risks, and the management of each risk shall be the sole responsibility of the business and corporate areas.

- 4.5. Large Risk Events or Risks unacceptable to ENEVA, which may jeopardize its perpetuity, reputation and values, shall include in their management initiatives of business continuity management, crisis management, as well as Risk sharing actions such as contracting insurance.

## **5. GUIDELINES FOR RISK MANAGEMENT**

### **METHODOLOGY**

- 5.1. The Company's Risk Management methodology is based on (but not limited to) internationally accepted standards, i.e., COSO-ERM model (*Enterprise Risk Management*) and ISO 31000.
- 5.1.1. **Risk Governance and Culture:** Risk culture shall be disseminated at all levels of the Company and the management and monitoring of Risks shall not be an exclusive action of a single executive or area. Managers are primarily responsible for the daily management of Risks associated with their area or business process and for disseminating a Risk management culture among their subordinates, managing exposure to Risks through action plans.
- 5.1.2. **Risk, Strategy and Definition of Objectives:** Risk strategy and management shall include internal and external factors, as well as the impact of Risks that may be at odds with the direction defined by the Company and may affect the success of the strategy or the achievement of business objectives.
- 5.1.3. **Identification, Assessment and Handling:** Risks shall be periodically identified, assessed, prioritized, and documented on a structured basis so that they can be properly handled. The Company shall be attentive to the arising of new and/or emerging Risks, which, when identified, shall be assessed, included in the Risk management process and, depending on their criticality, immediately reported and handled.
- 5.1.4. **Information, Communication and Reporting:** Information used for Risk management shall be complete and accurate, representing the current situation of the Company's operations, so that all employees understand their role within the control

structure and are provided with the necessary and assertive information for the performance of their activities and managing their risks. The Company's Risks shall be communicated and known by all those involved in their management and monitoring, and shall be reported on a timely basis. Risk communication process shall be clear and efficient, providing information in a format and time frame that enable Administrators and Employees to perform their responsibilities and make appropriate decisions.

- 5.1.5. **Monitoring** Risks shall be continuously monitored to prevent the Company's exposure to Risks from increasing and preventing business continuity. Appropriate monitoring of Risks consists of constant monitoring of the Company's control environment and risk response actions. Improvement actions shall be monitored, ensuring the achievement of the initial purpose, the implementation deadline and the effectiveness of risk reduction, if applicable. This assessment shall be performed at least every six months for Risks considered very high and high.

### **RISK MANAGEMENT GOVERNANCE STRUCTURE**

- 5.2. ENEVA adopts the concept of the three (3) Lines of Defense to implement its Risk management structure, seeking to ensure compliance with the defined guidelines.
- 5.3. **1st Line of Defense:** Is represented by all managers of the business and support areas, who shall ensure the effective management of Risks within the scope of their direct organizational responsibilities. It includes:
- a) Managing the Risks and controls of processes under their roles and relevant outsourced activities under its coordination, through preventive and detective approaches;
  - b) Implementing actions to mitigate and/or monitor Risks;
  - c) Communicating promptly to the areas of Governance, Compliance, Internal Controls and Risk Management whenever potential unexpected Risks are identified in the development of control activities or changes in standards and regulations in force;
  - d) Assessing external and internal standards and identifying the impact they may have on processes and procedures and the need for action plans to ensure adherence; and

- e) Defining and implementing action plans to address the notes made by areas with 2nd Line of Defense roles, by Audits and by Regulators.

5.4. **2nd Line of Defense:** Is responsible for supporting the 1st Line of Defense in managing Risks, and is represented by the areas of Governance, Compliance and Internal Controls and Risk Management, in addition to other corporate support areas with regulatory and advisory roles in matters directly related to risk management.

The areas of Governance, Compliance and Internal Controls and Risk Management are structures operating in consultation with the executive areas, but with independent assessment and reporting on Risk management and ENEVA's control environment.

The Governance, Compliance and Internal Controls area shall:

- a) Establish a set of practices and relationships between Shareholders, Board of Directors, Executive Board, Independent Audit and Statutory Audit Committee, with the purpose of improving the Company's performance and facilitating access in line with the interest of shareholders;
- b) Certify the efficiency and effectiveness of the control environment of the 1st Line of Defense, through monitoring and testing controls;
- c) Ensure the Company's Compliance and Internal Controls governance, through periodic monitoring and reporting.

The Risk Management area shall:

- a) Coordinate Risk Management activities with the business and corporate support areas;
- b) Develop and make available the methodologies, tools, systems, infrastructure and governance necessary to support Risk Management activities;
- c) Support the 1st Line of Defense in implementing effective Risk Management practices;
- d) Ensure Risk Management governance, through periodic monitoring and reporting;
- e) Coordinate crisis management activities and the development and implementation of business continuity plans;
- f) Work together with other corporate support areas that, among their duties, also have 2nd Line of Defense roles.

- 5.5. **3rd Line of Defense:** Is represented by Internal Audit, and aims to provide independent opinions to the Board of Directors, through the Statutory Audit Committee, on the Risk management process and the effectiveness of internal controls, having a structure and budget sufficient for the performance of its duties. It includes:
- a) Audit the Company's Risk management process with impartial, independent and timely opinions;
  - b) After implementation of action plans, audit the actions to ensure that they have all been implemented as planned;
  - c) Identify new weaknesses and processes suitable for prioritization based on the results of the Risk Assessment in progress;
  - d) Adjust the scope of the substantive or continuous monitoring testing environment based on the identification of new Risks or worsening of already identified Risks.

## **6. GENERAL PROVISIONS**

- 6.1. The Executive Board is responsible for defining the methodology to be used in the Risk management process and proposing the level of the Company's Risk Appetite to the Board of Directors. The Executive Board shall periodically monitor Risk management in order to ensure its effectiveness and the fulfillment of its objectives, reviewing this Policy and submitting adjustments and improvements for approval by the Board of Directors.
- 6.2. The Board of Directors is responsible for approving amendments to this Policy, authorizing, if necessary, any exceptions to the Policy, defining the level of Risk Appetite in conducting business and ensuring the Company's adherence to established Risk management policies and strategies.
- 6.3. The Board of Directors shall also seek to disseminate the risk management culture across the Company and ensure adequate and sufficient resources to the performance risk management on an independent, objective and effective basis.

## **7. REFERENCES**

- CVM Instruction No. 480/2009, dated December 7, 2009, as amended (“CVM 480”) and Novo Mercado Regulation of B3 S.A. – Brasil, Bolsa, Balcão (“Novo Mercado Regulation”);
- ERM (Enterprise Risk Management Framework) from COSO (Committee of Sponsoring Organizations of the Treadway Commission);
- ISO 31000, Risk Management — Principles and Guidelines, from ISO - International Organization for Standardization (“ISO 31000”)
- ENEVA's Bylaws;
- ENEVA's Code of Conduct.

## **8. ANNEXES**

Not Applicable.

**REVIEW AND APPROVAL**

Review	Date	Description of updates	
<b>0</b>	10/31/2018	Document creation.	
<b>1</b>	03/23/2023	Document review, updating information related to the 2nd and 3rd Lines of Defense	
Creation		Review	Approval
Luiz Amaral Risk Manager		Thiago Freitas Legal, Governance, Compliance and Internal Controls Officer	Board of Directors of ENEVA S.A.
<b>Review 1</b> Luiz Amaral Risk Manager		Marcelo Habibe Financial and Investor Relations Officer	Board of Directors of ENEVA S.A.

**KEY AUDIENCE**

- Members of the Board of Directors and Advisory Committees to the Board of Directors
- Board members (statutory or not);
- Chief Auditor;
- Governance, Compliance and Internal Controls and Risk Management Areas;
- ENEVA S.A. Employees