1. PURPOSE.

To establish principles, guidelines and responsibilities to be followed in the corporate risk management process, so as to enable the appropriate identification, assessment, treatment, monitoring and communication of the risks for which protection is sought and which may affect its strategic plan, in order to drive the risk appetite in the decision-making process in the pursuit of the fulfillment of its objectives, as well as the creation, preservation and growth of value.

2. SCOPE.

The Risk Management Policy applies to all business processes and transactions, except market risks, of Simpar S.A., its subsidiaries, affiliates and affiliates of the subsidiaries, hereinafter and jointly referred to as “Company” or ‘Simpar’.

3. SUMMARY.

4. DEFINITIONS.

The definitions below reflect The Company's views:

Company: encompasses Simpar, its subsidiaries and its affiliates, the affiliates of subsidiaries.

Director: represented by Officers, whether statutory or not, General Managers, Managers, Coordinators and any other person who holds a position other than those mentioned above, and who has a management function.

Control Objectives for Information and Related Technologies (COBIT): The Company refers to and uses as a model for information technology risk management the “Control Objectives for Information and Related Technologies” (COBIT). (Control Objectives for Information and related Technology - COBIT), which is a model of good practices created by ISACA (Information Systems Audit and Control Association) for corporate governance and management of information technology. corporate governance and management.

Enterprise Risk Management Integrating with Strategy and Performance: framework developed in 2017 by COSO - Committee of Sponsoring Organizations of the Treadway Commission, establishes a management methodology for Enterprise Risk Management.

Internal Controls: internal control is a process conducted by the Company's governance structure and management, and developed to support decisions with a higher level of security, reliability, integrity, efficiency and effectiveness, based on the objectives set by the Company, as well as its risk appetite. They are operationalized through a set of interconnected activities, plans, routines, methods and procedures, showing any deviations throughout management until the set objectives are achieved.

Risks: uncertain events of internal or external origin which may have a negative (threat) or positive (opportunity) effect on the fulfillment of the Company's objectives. It is the probability of something happening.

Risk factor: is the root cause of a given risk; it is the very event that gives rise to the occurrence of a risk.

Strategic risks: risks associated with the Company's strategic decisions to achieve its business objectives and/or arising from the Company's lack of capacity or ability to protect itself or adapt to changes in the environment. Strategic risks include the inability to raise sufficient financial resources to cover all planned investments and to finance its expansion strategy.

Operational risks: risks arising from inadequacy, failure, deficiency or fraud in internal processes, people or the technology environment, or related to situations of force majeure, which may hinder or prevent the achievement of the Company's objectives. These risks are associated with the performance of the Company's activities (related to its corporate objects), as well as other administrative support departments. Operational risks include significant impacts from cyber security incidents, systems failures, lack of computerization in processes and unfavorable decisions in judicial and/or administrative proceedings.

Market risks: risks defined as the possibility of losses resulting from movements in the market value of positions held by the Company, including the risks of transactions subject to exchange rate variations, inflation, interest rates, share prices and commodity prices. The Company sets its own rules for this type of risk in its Market Risk Management Policy.

Liquidity risks: risks defined as the Company's ability to meet its obligations within the agreed deadlines, including those arising from guarantees, without affecting its day-to-day operations and without incurring significant losses.

Credit risks: the possibility of losses associated with the financing granted to clients in the operation of the business (default), in addition to the counterparty risks assumed in treasury operations (financial investment, loan, debt management, collection and recovery).

Image risks: risks arising from internal practices, other risks and external factors which could lead to a negative perception of the company by clients, shareholders, investors, business partners and other stakeholders ("third parties"), in short, risks that could damage the reputation, credibility and brand of the Company, with consequent significant financial losses.

Compliance risks: risks arising from non-compliance with the laws and regulations applicable to the Company's business, mainly, but not limited to, Law No. 12846/2013, known as the Anti-Corruption Law, and its respective regulations - Decree No. 11129/22 and Law No. 13709/2018 - the General Personal Data Protection Law, which may result in financial loss through the payment of fines, indemnities, as well as damage to The Company's image and credibility in the market. Compliance risks include the possibility of the Company's subsidiaries being unable to obtain or renew their licenses and permits for their respective operations.

Social and Environmental Risk: risks related to relevant social and environmental issues and processes; potential damage to the environment, social relations and communities related to the economic activities of companies controlled by the Company.

Framework: basic structure supporting the concepts; models.

Self Assessment: method used to identify risks, exposures, vulnerabilities and action plans in relation to managers' perceptions and responsibilities.

Action plans: actions aimed at creating, correcting and/or improving the management of processes, people and systems in the realization of the Company's strategies, with a focus on managing the causes of risks. There must be a person responsible and a date for completion.

Probability: possibility of the risk materializing.

Impact: consequences in which the risk, if materialized, will affect the Company.

Risk matrix: graphic representation of the impact versus probability of the risks identified by the Company.

Inherent risk: the degree of risk intrinsic to the business operation or activity, without taking into account the implementation of the controls that mitigate it.

Residual risk: the level of risk taking into account risk mitigation actions and the result of testing control activities.

Risk appetite: the level of exposure to risk that the Company is willing to accept in order to achieve its strategic objectives.

Risk Tolerance: acceptable level that the organization is willing to bear for the impact that a given risk may cause.

Relevant Processes: processes that impact the Company's business, in the view of the Directors.

5. REFERENCE DOCUMENTS.

a) Control Objectives for Information and related Technology (COBIT);
b) Enterprise Risk Management Integrating with Strategy and Performance (COSO - 2017);
c) Law No. 6404/1976;
d) CVM Instruction 480/09;
e) CVM Instruction 586/17;
f) The Company's Code of Conduct.

6. GENERAL PRINCIPLES.

Control and risk management activities must be carried out at all levels of the Company and at all stages of corporate processes.

The processes, procedures and internal controls must enable Management and the other managers involved to manage the risks in accordance with the applicable laws, policies and the limits (appetite) established by the Company, which are validated by the Audit Committee and approved by the Board of Directors, seeking an environment of continuity and sustainability of the Company's business.

7. METHODOLOGY USED.

The Company's risk management process was set based on the Risk Management methodology coordinated by COSO, version 2017 (Committee of Sponsoring Organizations of the Treadway Commission) in conjunction with COSO's Integrated Internal Controls Management - 2013, considering integration with the ISO 9001 and ISO 31000 standards, as well as seeking to adapt the governance and management of information technology in line with COBIT (Control Objectives for Information and Related Technologies). (See comment on COBIT above).

7.1 STAGES OF RISK MANAGEMENT.

1ª) Identifying Risks: defining the set of external and/or internal events that may affect the Company's objectives, including those related to intangible assets. This process must be continually improved and reviewed, even in the face of changes to the Company's objectives and consequent risks. The risk identification approach used by the Company is Self Assessment and process mapping, based on interviews with the managers and officers of each of the Company's business lines, with a view to the main processes for which they are responsible. The product of this identification is a comprehensive list of risks that could threaten the achievement of the Company's business objectives. The risks to which The Company is subject must be documented and formalized in a structured manner so that they are known and dealt with appropriately, and their nature and origin are categorized as follows: (i) strategic risks; (ii) operational risks; (iii) market risks; (iv) liquidity risks; (v) credit risks; (vi) image risks; (vii) compliance risks and (viii) social and environmental risks.

2ª) Risk Analysis/Classification: this stage involves those directly responsible for carrying out the respective acts or actions verifying the causes and consequences of the risks, as well as the likelihood of these consequences occurring. The Officers, the Audit Committee and the Board of Directors, each within the scope of their authority, must analyze risk events according to their impact, taking into account three (3) levels: high, medium and low, and their probability of occurrence, considering five (5) categories: financial, business, HSE (health, safety and environment), reputation (image), compliance.

The impact and probability matrix for each of the subsidiaries must be reviewed annually by the CFO and the CEO, in accordance with the specifics of their business, and the review must be validated and approved by the Audit Committee.

This matrix must be taken into account in order to comply with the scope of the Internal Audit and Internal Controls, taking into account the integrated view of the risk.

Once the impact and probability matrix is reviewed, the Internal Controls, Risks and Compliance Department will reclassify the criticality of the mapped risks according to the new matrix and report the risks that are reclassified as “high” to the Audit Committee, which in turn will report them to the Board of Directors.

The Directors must assess risk events by their impact and probability of occurrence, considering the relevance of the 5 risk categories mentioned above, their financial and/or other consequences, whether quantifiable or not. The result of the risk assessment between probability versus impact of occurrence is represented in the risk matrix (3x3 matrix), where the data on perceived impacts and probabilities are inserted into the matrix which will calculate the inherent risk according to the result of the effectiveness test of the controls defined to mitigate these risks, as shown below:

R = PXI		**Probability**		
		Low	Medium	High
Impact	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Once the risks have been identified and assessed, they will be prioritized according to the highest ratio between impact and probability, thus establishing the level of exposure to risk which will guide the priority of periodic monitoring. By doing thos, the risk assessment provides a map of the company's risks, providing a mechanism for prioritizing these risks and, consequently, a tool for directing efforts to minimize the most significant risks by means of an internal control structure aligned with the company's objectives.

3ª) Risk treatment: after the risk assessment, the treatment of the risks is set, as well as how they should be monitored and communicated to the different parties involved. Treating risks consists of deciding whether to avoid, mitigate, share or accept them. The decision depends mainly on the company's degree of risk appetite, which is defined by management and validated by the Board of Directors. The Directors must determine how to respond to the risks identified and it is the responsibility of the Internal Controls, Risks and Compliance Department to support them in defining the action plans needed to deal with the risks and to monitor the implementation of these plans, reporting to the Audit Committee any delays in complying with them.

In addition, the acceptance of residual risks must be assessed by the Audit Committee and validated by the Board of Directors, in line with the Company's risk appetite level. Once this flow has been met and the risk accepted, the acceptance must be formalized.

4ª) <u>Risk monitoring:</u> ensuring the effectiveness and adequacy of the internal controls established and obtaining information that will improve the risk management process, through continuous and impartial assessments. It is the responsibility of the Directors and the Board of Directors to ensure the effectiveness and adequacy of the internal controls established and to obtain information that will lead to improvements in the risk management process, by means of continuous and impartial evaluations. In addition, the main monitoring activities include risk consolidation reports, reconciliations, inventories, audits, self-assessments, monitoring the status of action plans and continuous verification.

5ª) <u>Information and communication:</u> communicating the results of all stages of the risk management process clearly and objectively to all stakeholders, contributing to an understanding of the current situation and the effectiveness of action plans.

6ª) <u>Reviewing the risk map:</u> every year the risk and control matrices for the processes relevant to the company's business must be reviewed by the responsible manager, who must substantiate/justify any changes in relation to the previous matrix. Without prejudice to this, the risk matrix must be reviewed in its entirety every three (3) years or whenever required, by means of a self assessment.

7ª) <u>Reporting</u>: following the governance structure, the Risk Map must be reported to the structures provided for in this policy and in the manner determined.

8. RISK MANAGEMENT INSTRUMENTS

The main instruments used by the Company to protect risks are made up mainly of the following, according to the steps defined in the section above:

i. Identification of risks through Self Assessment and process mapping, which consists of interviews conducted by the Internal Controls, Risks and Compliance Department with process managers and other areas involved.

Assessment and analysis of risks through the perception of impacts and probabilities of occurrence with the company's managers, classifying them using qualitative factors such as “low”, “medium” or “high”. The data is then entered into the 3x3 risk matrix, which calculates the inherent risk;

ii. Treatment of risks through:

a. Classification and alignment with the strategy for drawing up the internal controls work plan in the selected departments;

b. Selection of one or more options for treating the risks and the subsequent implementation of controls and/or a follow-up process;

c. Defining the action plans needed to treat the risks and monitoring them using the Company's Risk Management tool, which will send alerts to those responsible;

d. Governance structure (Management, Audit Committee and Board of Directors) for monitoring action plans and directing work.

iii. Monitoring the risks affecting the Company through:

a. Indicators showing probability, impact, tolerance, residual and inherent risk obtained through the Company's Risk Management tool;

b. Testing the operational effectiveness of the internal controls that mitigate the company's risks, through samples that are selected according to the methodology described above.

In addition, the Audit Committee and the Board of Directors are responsible for monitoring internal controls and risk management, assessing the effectiveness and progress of the actions proposed by managers as a way of mitigating or eliminating risks.

As a result of the whole process, the Company may adopt one of the following alternatives to treat the risks:

i. Accept: accept that the risk may occur and decide how to deal with it if it materializes;

ii. Avoid: modify the actions planned to avoid the risk;

iii. Mitigate: actions are taken to reduce the likelihood of the risk materializing and/or its severity;

iv. Sharing: activities aimed at reducing the probability of the risk occurring and/or its severity, by transferring or sharing part of the risk to third parties.

9. RISK MANAGEMENT ORGANIZATIONAL STRUCTURE.

The company separates departments, roles and professionals, defining the responsibilities of each one and setting limits for these responsibilities.

The organizational structure of subsidiaries may vary, always following the law and regulations applicable to the type of company, so the Company may not have a Board of Directors or an Audit Committee. In these cases, the duties will be carried out by the Controlling Company's bodies.

10. RESPONSIBILITIES AND DUTIES

10.1 THE BOARD OF DIRECTORS

The Board of Directors is the central body of the governance system and is responsible for the Company's longevity and the creation of long-term value in an assertive and transparent manner. Therefore, the Board of Directors is responsible for periodically assessing the risks to which the Company is exposed, the effectiveness of the risk management systems, internal controls and the integrity/compliance system.

The Board of Directors is also responsible for:

i. ensuring that the Board of Directors has mechanisms and internal controls in place to understand, assess and control risks in order to keep them at levels compatible with the established limits, including an integrity/compliance program aimed at complying with laws, regulations and external and internal standards;

ii. validating the Company's risk appetite level approved by Management;

iii. ensuring that the Audit Committee has its own budget for hiring consultants for accounting, legal or other matters, when the opinion of an external specialist is required;

iv. approving this policy and future reviews;

v. approving the duties of the Internal Audit department.

10.2 DIRECTORS

Management is responsible for acting directly in risk management, understanding and taking responsibility for the following stages: identification, assessment, treatment and monitoring.

Therefore, considering the role of managers in the process of risk management and internal controls, the Board of Directors is responsible for:

i. ensuring the implementation of the action plans set for dealing with risks;

ii. assisting the Internal Controls, Risks and Compliance Department in the processes of identifying and developing risk portfolios, responding to risk self-assessment questionnaires and enabling the mapping of the processes under its responsibility;

iii. developing and implementing action plans for the failures, absences and insufficiencies identified within the appropriate timeframe for each note formalized by the Internal Controls, Risks and Compliance Board;

iv. justifying the impossibility of complying with an action plan and/or delay in complying with one;

v. justifying any assumptions of risk for validation by the governance structure;

vi. providing clarification on the conduct of risk management under their responsibility to the Audit Committees, whenever requested;

vii. providing the necessary updates on the risks of its activity to the Internal Controls, Risks and Compliance Board.

10.3 THE EXECUTIVE BOARD

The Executive Board is responsible for ensuring and facilitatating access for members of the Board of Directors, the Committees (whether statutory or not), the Fiscal Council, the internal and external audits and the advisory bodies, to the Company's premises and to the information, files and documents demonstrably necessary for the performance of their duties.

10.4 STATUTORY AUDIT COMMITTEE

The Statutory Audit Committee must operate in accordance with its Internal Regulations and is responsible for supervising the quality and integrity of financial reports, adherence to legal, statutory and regulatory standards, the adequacy of risk management processes and the activities of the internal audit and independent auditors.

By delegation from the Board, the Audit Committee monitors these issues:

- **i.** give an opinion on the hiring, assessment and dismissal of independent auditing services;
- **ii.** evaluate the quarterly information, interim statements and financial statements;
- **iii.** evaluate and provide opinions on the internal control report issued by the independent auditors and propose recommendations to management and the Board of Directors;
- **iv.** monitor the activities of the Company's Controls, Internal Risks and Compliance Department, and may receive or request reports from the Controls, Internal Risks and Compliance Department on the execution and compliance with the Company's Compliance Program. Advising the Board on the effectiveness of activities and proposing recommendations, whenever necessary, regarding activities, structure, qualifications and budget for consideration by the Executive Board and the Board of Directors;
- **v.** advise the Board of Directors on risk management and monitoring risk exposures, in accordance with the Company's Risk Management Policy;
- **vi.** evaluate, monitor and recommend to management the correction or improvement of the Company's internal policies, including the policy on transactions between related parties, the Risk Management Policy, the Code of Conduct, the other regulations of the Company's Compliance Program;
- **vii.** receive and process information about non-compliance with legal and regulatory provisions applicable to the Company, as well as internal regulations and codes, including potential violations of Law No. 12846/2013 - the Anti-Corruption Law - and other laws prohibiting practices of bribery, fraud, offering or receiving an undue advantage, as well as recommending and verifying the application of disciplinary measures by the responsible areas, or, in the case of complaints against Company officers, by the Board of Directors;
- **viii.** prepare a summary annual report, to be presented exclusively to the Board of Directors, containing a description of: (a) its activities, the results and conclusions achieved and its recommendations; and (b) any situations in which there is a significant divergence between the company's management, the independent auditors and the Audit Committee in

relation to the company's financial statements;

ix. monitor and assess whether transactions with related parties are being carried out under market conditions, under the terms of the Company's current policy on transactions with related parties;

x. In order to carry out its duties, the Audit Committee shall have operational autonomy and a budget, within the limits approved by the Board of Directors, under the terms of the Company's Bylaws;

xi. Annually evaluate the structure and budget of the Internal Audit department to ensure that they are sufficient to perform its duties;

xii. Report the results of the activities of the Internal Audit department to the Board of Directors.

10.5 INTERNAL AUDIT

The Internal Audit has the following duties

i. monitor the quality and effectiveness of risk management and governance processes, as well as the Company's internal controls and compliance with the rules and regulations associated with its operations;

ii. provide the Audit Committee with independent, impartial and timely assessments;

iii. consolidate, assess, monitor and communicate the Company's risks to the Audit Committee;

iv. assess the quality and effectiveness of the company's risk management, control and governance processes.

Internal Audit must report its activities to the Audit Committee, which in turn reports to the Board of Directors. As an alternative to setting up its own Internal Audit department, the company may hire an independent auditor registered at the CVM to perform this role.

10.6 INTERNAL CONTROLS, RISKS AND COMPLIANCE DEPARTMENT

The Company will make the Internal Controls, Risks and Compliance Board responsible for leading the work of monitoring compliance risks with the aim of identifying, mitigating and preventing strategic, operational, image, socio-environmental and compliance risks, as well as guiding company employees and third parties on the Company's internal rules.

Its main duties are:

i. monitor non-compliance with applicable laws and regulations;

ii. update the Code of Conduct guidelines whenever necessary and disseminate them among employees;

iii. update the guidelines of the Third Party Code of Conduct whenever necessary and disseminate them;

iv. Inform the Ethics and Compliance Committee of: a) situations that characterize a compliance and image risk for the Company, b) information on complaints received through the Whistleblower Channel and the status of investigations in accordance with the matrix approved by the Audit Committee; c) suggestions for changes to the Company's Anti-Corruption Policies; d) any non-compliance with the Company's Anti-Corruption Policies and validating the application of disciplinary measures for said non-compliance; e) information on donations and sponsorships to Public Administration agencies for validation;

v. evaluate, investigate and deal with complaints received by the outsourced company that manages the Company's channel which deal with (i) misconduct, (ii) non-compliance with the Code of Conduct, Anti-Corruption Policies or other Company procedures; (iii) situations to conflicts of interest;

vi. report on the status of action plans for preventive actions and the application of disciplinary measures;

vii. support the managers in defining the action plans needed to deal with risks and ensure that these plans are implemented

viii. support the legal department in assessing the compliance sections in the company's contracts;

ix. assess and point out the risks for validation by the board of directors of the obligations involving compliance imposed by clients and third parties.

The Company's Internal Controls, Risks and Compliance Department reports to the company's Audit Committees and has the Ethics and Compliance Committee as an advisory body, in accordance with its respective duties and must annually submit the Risk Map to the Board of Directors for information.

10.7 FINANCIAL COMMITTEE

The Finance Committee is a non-statutory body that advises on the assessment of financial risks in accordance with the appropriate governance structure. Management, supported by the Finance Committee, recommends actions to the Board of Directors so that activities which result in financial risks are governed by appropriate practices and procedures. This committee is made up of at least three (3) and at most five (5) members, elected and dismissed by the Board of Directors.

10.8 ETHICS AND COMPLIANCE COMMITTEE

This is a non-statutory, permanent body of the Company, whose purpose is to advise the Audit Committee, the Executive Board and the Company's Internal Controls, Risks and Compliance Role:

- **i.** complying with, disseminating and updating the Company's Code of Conduct and internal rules;
- **ii.** recommending and monitoring preventive actions for cases of violation of national laws applicable to the Company's business, especially compliance with Law No. 12846/2013 - the Anti-Corruption Law - and other laws prohibiting practices of bribery, fraud, offering or receiving an undue advantage;
- **iii.** evaluating the efficiency and effectiveness of the legal requirements of the Integrity Program, required by Decree No. 8420/2015 and other rules of the Ministry of Transparency, Supervision and the Office of the Federal Controller General - CGU, with a view to entrenching a culture of compliance, mitigation and prevention of risks and losses;
- **iv.** validating suggestions for changes to the Company's Anti-Corruption Policies;
- **v.** validating requests for donations and sponsorships from public administration agencies;
- **vi.** evaluating relevant cases involving the actions and omissions of the Company's employees and third parties, suppliers, service providers, partners and business consultants who have a relationship with the Company;
- **vii.** monitoring the indicators related to the Compliance Program and suggesting improvements and adjustments to the results identified.

11. VIOLATIONS TO THIS POLICY

Any violations to the terms of this policy will be assessed by the Board of Directors, which will define the application of the appropriate measure(s). In the event of non-compliance by members of the Board itself, the members of the Audit Committee should be involved.

12. FINAL PROVISIONS.

This policy shall be reviewed whenever necessary, and its reviews shall be submitted to the Audit Committee and the Company's Board of Directors.

Any stakeholder may propose to review the contents of the policy.