RISK MANAGEMENT POLICY OF BRISANET SERVIÇOS DE TELECOMUNICAÇÕES S.A.

The activities of Brisanet Serviços de Telecomunicações S.A. (“**Company**”) and its direct and indirect subsidiaries comprise primarily the trade and provision of services in the telecommunications and technology sectors. This Company Risk Management Policy (“**Policy**”) describes the way in which the Company manages the Risks (as defined below) to which it is subject.

1 PURPOSE

1.1 This Policy establishes the principles and parameters to be observed in relation to the Company's risk management process with a view to identifying, assessing, prioritizing and managing risks.

1.2 This policy also describes the risk management process, the communication procedures and the responsibilities of the Company's main bodies.

2 SCOPE

2.1 This Policy is binding on all departments, collaborators, management and employees of the Company. The Company’s subsidiaries controlled and affiliated companies must also comply with the provisions set forth herein.

3 REFERENCES

3.1 The following documents should be taken into consideration for the application and interpretation of the terms of this Policy:

(i) COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework;

(ii) Recommendations of the Brazilian Institute of Corporate Governance (“**IBGC**”);

(iii) Regulation of the Novo Mercado Novo Mercado of B3 S.A. – Brasil, Bolsa, Balcão (“**Novo Mercado Regulation**” and “**B3**”, respectively);

(iv) The Company’s Risk Appetite Statement (RAS);

(v) The Company’s Risk Management Manual;

(vi) The Company’s Code of Ethics;

(vii) The Company’s Anticorruption Policy;

(viii) The Company’s Information Disclosure Policy;

(ix) The Company’s Securities Trading Policy; and

(x) The Company’s Policy on Transactions with Related Parties.

4 DEFINITIONS

“**Risk Appetite**”	*Risk Appetite Statement* (“**RAS**”) means the level of risk that the Company is willing to take considering its ability to assume risks.

The RAS establishes the exposure limit of risks that are acceptable and those considered unacceptable by the institution and is prepared considering its strategic objectives;

“**Internal Audit**” refers to the area of the Company that performs the third line of defense of Risk Management, independently reviewing and evaluating its risk management and the effectiveness of its internal controls;

“**Compliance**” in this Policy means the area that carries out the second line of defense of Integrity Risks, acting in a segregated and independent manner in relation to the business areas and in support of the Audit Committee;

“**Internal Controls**” refers to policies, standards, procedures, activities, and mechanisms designed to ensure that business objectives are met and that undesirable events are prevented or detected and corrected;

“**Integrity risk**” means the Risk associated with legal or regulatory sanctions, financial or reputational loss, resulting from any failure to comply with laws, agreements, regulations, the Code of Ethics and/or the Company's internal policies or rules. It includes the risk of fraud and sabotage in the Company's processes, misappropriation of assets or any type of corruption;

“**Information Technology Risk**” means the risk associated with failure or misuse of the information technology environment, including loss, misuse or unauthorized disclosure of sensitive personal data or confidential information of internal or external shareholders;

“**Strategic Risk**” means the risk associated with the company's strategy for generating and protecting value and derives from changes in the external environment, the market, competitors, mergers and acquisitions, innovations, technologies and the portfolio of products and/or services; as well as the efficiency of management in relation to finance (generation of operating cash flow, profitability, indebtedness, leverage, application and raising of financial resources), image, reputation and operations (organizational culture, management of people, processes and other resources);

“**Financial Risk**” means the Risk relating to the Company's financial capacity, whether in relation to liquidity, exposure to exchange rate variations, compliance with financial restrictions in financing contracts and the Risk of customer default due to the lack of financial capacity to honor their debts, disagreements between the Company and its debtors over the amounts owed and others;

"**Operational Risk"**	means the risk of failure, deficiency or inadequacy of internal processes, people or systems, including the legal risk associated with inadequacy or deficiency in contracts entered by the Company, sanctions due to non-compliance with legal provisions, compensation for damages to third parties arising from the Company's activities, inadequate practices relating to clients, products and services, and relating to the inefficiency of the Internal Controls environment;
"**Risk**"	means the uncertainty related to certain events and their potential outcome that could have a significant effect on the Company's activities. All business activities may represent some risk arising from potential threats or the non-realization of opportunities, which may hinder, prevent, affect or interfere with the achievement of its objectives.
"**Risk & Internal Controls**"	means the area that carries out the second line of defense in the management of Strategic Risk, Operational Risk and Information Technology Risk, acting in a segregated and independent manner in relation to the business areas and in support of the Audit Committee.

5 RISK MANAGEMENT PROCESS

5.1 The Company classifies its risks according to the following categories:

(i) Strategic risks;

(ii) Financial risks;

(iii) Integrity risks;

(iv) Operational risks;

(v) Information technology risks.

5.2 Risk management comprises the process of assessing and responding to risk related to the Company's business with the aim of reducing such exposures to acceptable levels.

5.3 Risk management is a crucial element of the Company's strategies, as it provides a systematic process for identifying Risks related to new, current and future business activities. Risk control activity involves the categorization and assessment of each Risk and the application of management controls to mitigate the Risk, based on a judgment about the likely impact if no action is taken, combined with an assessment of the likelihood of reoccurrence of the risk.

5.4 The company's risk management process considers its strategic planning in line with the level of risk it is willing to accept (Risk Appetite) in the execution of its strategy and operations.

5.5 The steps of the Risk Management process are:

(i) establishment of context/strategy: understanding of the Company's history, capturing the strategic and operational objectives, the internal and external environment in which it operates and its *stakeholders* (interested parties);

(ii) risk identification: mapping and identification of risks, classified according to their category. The risks are mapped based on the perception of the Company's management bodies, executives and employees, as well as based on external sources (auditors, government, media, regulatory bodies and other interested parties);

(iii) risk assessment: analysis of previously identified risks, by verifying their origin, causes and consequences, being evaluated according to their impact and probability of occurrence. The relationship between the impact and the probability of occurrence gives rise to the final risk rating (final risk rating);

(iv) prioritization and treatment of risks: based on the result of the classification of the final risk rating, the risks considered most critical are prioritized and a treatment is defined for each risk. The treatment of risks consists of a response action, according to the Company's risk appetite;

(v) monitoring the response actions implemented and evaluating their effects on residual exposure to risks, monitoring the performance of risk indicators and seeking continuous improvement.

5.6 Once the impact and probability relationship has been established, the final risk rating can be: (i) low; (ii) medium; (iii) high; or (iv) critical.

5.7 Following this assessment, the Company will adopt one or more of the following possible actions to deal with the Risks:

(i) avoid/eliminate discontinuation of the activities that generate the Risk;

(ii) mitigate: the adoption of initiatives or establishment of control(s) to reduce the probability and/or impact of the Risk;

(iii) transfer/share: reducing the likelihood and/or impact of Risks by transferring or assigning part of the Risk, in which case the Risk will only be monitored;

(iv) explore: increase exposure given an expected return.

5.8 The Company's risk profile is monitored monthly by the Risk Committee, reporting directly to the Executive Board, quarterly by the Audit Committee and every six months by the Board of Directors. This monitoring aims to ensure the effectiveness and adequacy of the risk response actions defined as treatment for each of the identified risks and to obtain information that provides improvements in the Risk Management process.

5.9 The results of the monitoring process must be communicated to each level of management by means of reports consolidated by the Risks and Internal Controls area, with the support of each Risk owner.

5.10 To safeguard the Company, its activities and objectives, protection instruments shall be established that are constantly monitored, reviewed and improved, which must comply with the Risks listed in this Policy

6 GCRISIS MANAGEMENT, CONTINGENCIES AND BUSINESS CONTINUITY PLANS

6.1 The contingency and crisis management plans consist of response measures and actions to be taken by the Company when any risk event materializes. These plans aim to get the Company's fundamental processes back into full operation, or in a minimally acceptable state for the sustainability of operations, as quickly as possible, avoiding a prolonged stoppage and extension of losses. Crisis management plans define the roles and responsibilities of the teams involved in triggering contingency actions, before, during and after the occurrences.

7 RISK MANAGEMENT STRUCTURE

7.1 Risk management is the responsibility of all management and employees and requires the active participation of all areas of the Company, to the extent of their competencies, integrating with the strategic goals and objectives of the business of the Company and its controlled companies.

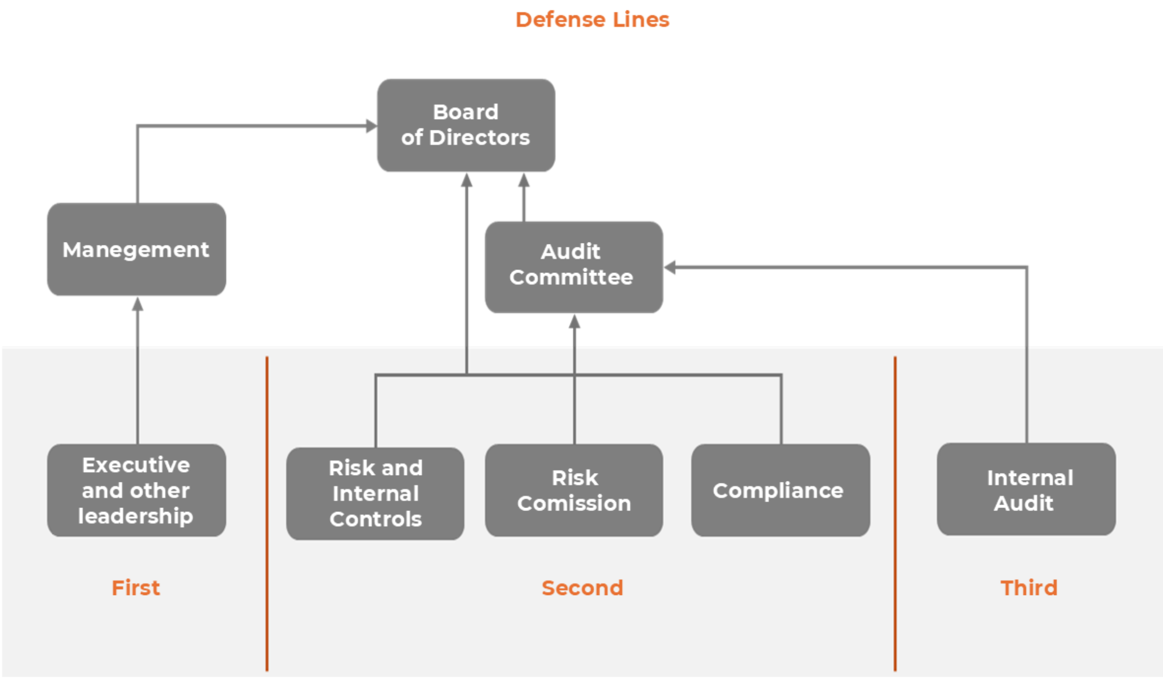
7.2 The Company adopts the concept of 3 (three) lines of defense to operationalize its risk management structure, to ensure compliance with the guidelines, as follows:

(i) <u>first line of defense</u>: comprised of all management personnel in the business and support areas, who must ensure effective Risk management within the scope of their direct organizational responsibilities;

(ii) <u>second line of defense:</u> comprised by the departments of Corporate Governance, Compliance, Risks and Internal Controls, which act in a segregated and independent manner in relation to the business and support areas and the Audit Committee. The second line of defense analyzes and evaluates the Risks and reports them directly to the Board of Directors, or through its support committees; and

(iii) <u>third line of defense</u>: constituted by the Internal Audit area and whose objective is to provide independent opinions on the Company's Risk Management and the effectiveness of the Company's internal controls environment.

7.3 These lines of defense are structured as follows, observing the roles and responsibilities described in item 8 of this Policy:



8 ROLES AND RESPONSIBILITIES

8.1 **Board of Directors**. The Company's Board of Directors is responsible for:

(i) review and approve the Company's Risk Appetite Statement and this Policy, in order to establish a risk management culture aligned with the business strategy;

(ii) monitor the Risk management strategy and activities and the exposure response system;

(iii) ensure that the risk management function has sufficient resources, including people, processes and technology, to fully carry out its functions; and

(iv) make the main decisions regarding the Company's risk management process, including those that may affect the Company's risk profile or exposure.

8.2 **Audit Committee.** The Company's Audit Committee is responsible for:

(i) advise the Executive Board and the Board of Directors, monitoring, examining, evaluating, informing and recommending improvements in the adequacy of the internal environment and effectiveness of the Risk Management process;

(ii) supervise the activities of the Risk Committee with the support of periodic reports;

(iii) promote discussions about the Company's risk assessments, certifying that the impact exposure and probability are adequately dimensioned;

(iv) assess and monitor exposure to Financial risk and consumption of risk appetite, in accordance with the Company's Risk Appetite Statement (RAS); and

(v) periodically evaluate the Risk Management Policy and the Company's Risk Appetite.

8.3 **Executive Officers**. They are the risk owners:

(i) identifying, evaluating, monitoring and correcting any deviations, as well as monitoring Risks;

(ii) implement the Company's strategies approved by the Board of Directors with regard to risk management;

(iii) propose the Company's Risk Appetite to the Board of Directors;

(iv) conduct a periodic review of this Policy and submit any suggestions to the Board of Directors; and

(v) periodically evaluate the Risk assessment, reporting any findings to the Board of Directors.

8.4 **Executive Managements and Managements**. They are the executors of the risk mitigation plans:

(i) prepare the action plan together with the Board of Directors, implementing, monitoring, correcting and reporting the results;

(ii) employ a participatory management style and encourage employees to participate in decision making and discuss risks that affect business strategy and objectives;

(iii) discuss and evaluate changes in the internal and external scenario, report changes in the risks under its management and identify the potential impacts of new Risks;

(iv) communicate expectations of conduct for all aspects of risk management and seek support from the Risk Management area; and

(v) participate in the Risk Committee, when invited, to report risk events and their respective deviations from the approved risk appetite, as well as the respective action plans.

8.5 **Risk Commission**. The Risk Committee is responsible for:

(i) evaluate and recommend changes in the Risk Management policy and in the Company's risk appetite;

(ii) Periodically evaluate the strategic and operational risk matrices, based on a consolidated and integrated view of the Company's list of risks, recommending corrective actions to the Executive Board;

(iii) validate and prioritize risk response action plans, and ensure that action plans are properly implemented and are being effective in addressing the proposed risks; and

(iv) validate the revised Strategic Risk matrix based on strategic planning updates and changes in the business, prior to reporting to the Audit Committee and the Board of Directors.

8.6 **Risks and Internal Controls**. The Risks and Internal Controls area is responsible for:

(i) propose and implement guidelines, methodologies, processes and procedures for Risk Management, provided that the guidelines provided by this Policy and by the Audit Committee are respected;

(ii) coordinate and guide the internal workforce and the Company's business areas in carrying out and standardizing the exercise of their functions in the first line of defense of Risk Management;

(iii) propose and monitor the Company's risk management processes, under the terms of this Policy and, as applicable, the Company's other policies, with a view to the proper preparation of financial information;

(iv) review and consolidate the information and risk reports received from the Company's business areas, reporting them to the Risk Committee, the Audit Committee and the Board of Directors;

(v) meet the reporting demands of the Audit Committee, generating relevant information and operationalizing risk management activities; and

(vi) evaluate and monitor Strategic Risk, Operational Risk and Information Technology Risk.

8.7 ***Compliance***. The Compliance area is responsible for:

(i) Advise and support the Audit Committee in the execution of the strategy and in the activities of Integrity Risk Management;

(ii) Assess and monitor Integrity Risk; and

(iii) review and consolidate the information and reports on Integrity risks received from the Company's business areas, reporting them to the Risk and Internal Control area.

8.8 **Internal Audit**. The Internal Audit is responsible for:

(i) evaluating the effectiveness of Risk Management in order to contribute to the achievement of the Company's objectives, acting autonomously and independently, at all levels;

(ii) writing periodic reports to the Audit Committee; and

(iii) carry out evaluation and control tests on the Risk Management practices, identifying deviations and proposing improvements aimed at safeguarding the interests of the Company's shareholders.

9 GENERAL PROVISIONS

9.1 This Policy will be reviewed whenever there are relevant changes in the Risk Management processes or when the Board of Directors deems it necessary.

* * *

This is a free translation of Risk Management Policy of Brisanet Telecomunicações S.A.