INFORMATION SECURITY POLICY

OF

LIGHTROCK GESTORA DE RECURSOS LTDA.

APRIL 17, 2023

1. INFORMATION SECURITY POLICY

1.1. INTRODUCTION

LIGHTROCK GESTORA DE RECURSOS LTDA. is a limited liability business company with its principal place of business in the city of São Paulo, state of São Paulo, at Avenida Brigadeiro Faria Lima, No. 3477, suite 42-A, Postal Code (CEP) 04.538-133, Itaim Bibi, enrolled with the National Corporate Taxpayers' Register of the Ministry of Economy ("CNPJ/ME") under No. 27.927.837/0001-37 ("Manager"), accredited by the Securities Commission (" CVM ") for the professional exercise of securities portfolio management activities, in the asset manager category, pursuant to CVM Resolution No. 21 of February 25, 2021 ("CVM Resolution 21").

The Manager is a member of the Lightrock group ("Lightrock Group"), a global asset and securities management group, which acts as a manager of specialized investment funds and other investment vehicles, which invest in a wide range of sectors, geographic locations, classes of assets, and investment strategies.

In view of the nature of the management activities it develops, the Manager is subject to extensive legislation, regulations, and self-regulations in the Brazilian market. In order to fully meet the requirements of the applicable legislation, regulations, and self-regulation, as well as adapt its activities to the best market practices, the Manager adopts the following internal policies: (i) code of ethics and conduct; (ii) securities trading policy; (iii) risk management and liquidity management policy; (iv) business plan; (v) this Information Security Policy (as defined below); (vi) order division and sharing policy; (vii) compliance and internal controls policy; (viii) policy on the prevention of money laundering, terrorism financing, and the proliferation of weapons of mass destruction ("PLD/FTP") (collectively, the "Internal Policies").

All members, officers, managers, and employees of the Manager directly involved in securities portfolio management activities ("Collaborators"), linked to the Manager on the date of preparation of the Internal Policies and/or who become part of the Manager's team in the future shall receive a copy (in printed and digital versions) of the Internal Policies.

The Manager establishes this information security policy ("Information Security Policy") in order to establish the principles, concepts, and values that shall guide the Manager's information security in its internal performance and with the market, as well as in its relationships with different publics.

Its purpose is to ensure that the organization's information is being treated appropriately to guarantee the Confidentiality, Integrity, and Availability criteria, as defined below.

In addition, it describes the conduct deemed appropriate for the handling, control, and protection of information against destruction, modification, undue disclosure, and unauthorized accidental or intentional access.

The principles and rules of this Information Security Policy shall be observed by all Collaborators of the Manager.

Upon receiving a copy of this Information Security Policy, the Collaborators shall sign an instrument of adhesion, in accordance with the form in Exhibit I to the Compliance and Internal Controls Policy of the Manager ("Instrument of Adhesion").

The Collaborators may also consult this Information Security Policy at the Manager's electronic address: www.lightrock.com.

This Information Security Policy shall be updated at least every three years by the Manager's Compliance, Risk, and PLD/FTP Officer, in order to contemplate any amendments to the applicable legislation, regulations, self-regulations, and best practices. Whenever this Information Security Policy is updated, the Collaborators shall receive a new copy of the updated Information Security Policy (printed and scanned), and shall sign a new Instrument of Adhesion.

The Instrument of Adhesion signed by Collaborators shall be scanned and filed by the Compliance, Risk, and PLD/FTP Officer, and they shall be kept for the entire period of professional relationship with the Collaborator and for an additional period of at least five (5) years as from the Collaborator's termination date, for any reason.

In addition to reading this Information Security Policy, all Collaborators shall read and understand the group of rules applicable to the Manager in the legal, regulatory, and self-regulatory scope. In case of doubts about the rules to be analyzed and/or regarding the interpretation of the content of these rules, the Collaborators shall contact the Compliance, Risk, and PLD/FTP Officer for the necessary clarifications.

The provisions of the Information Security Policy shall be construed in an integrated manner by the Collaborators, who shall consider the group of internal policies of the Manager, as well as the applicable legislation, regulations, self-regulations, and best market practices.

Organizational Structure of the Manager

The Manager was organized to act in securities portfolio management and its organizational structure is divided into two (2) distinct areas, namely: (i) fund management, and (ii)

compliance, risk management, and PLD/FTP. The Manager establishes and develops mechanisms to guarantee the independent performance of all areas.

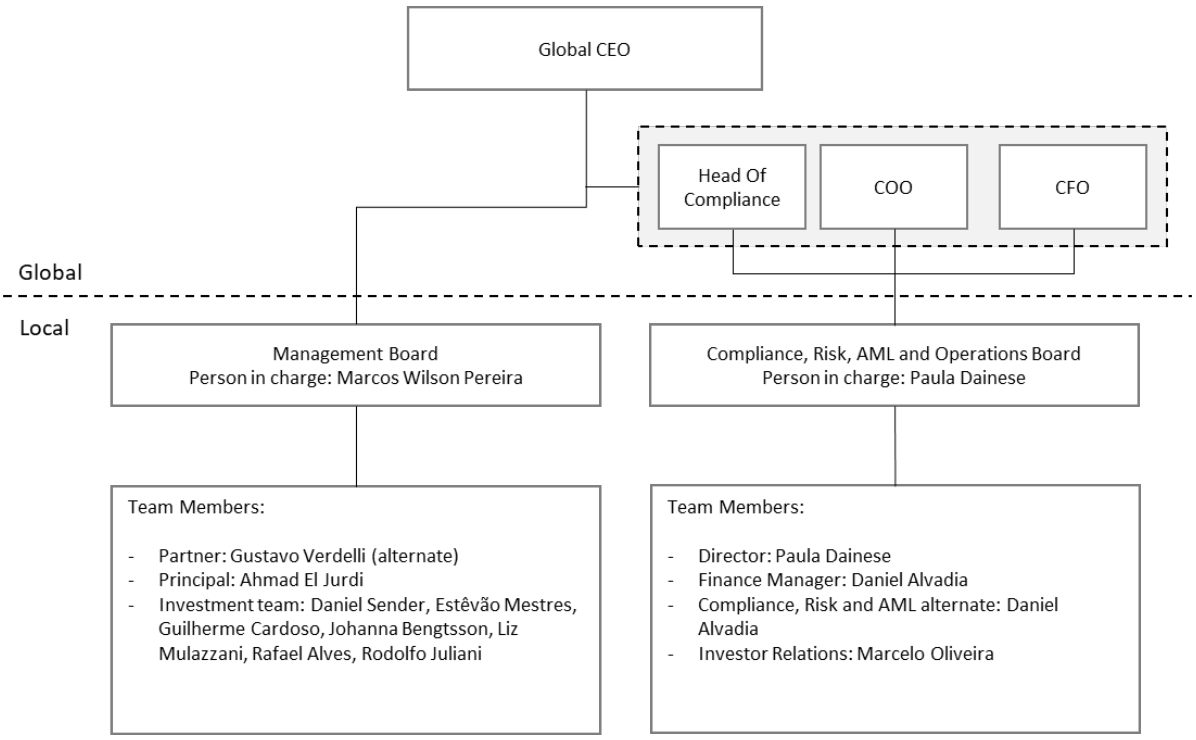
The main duties of each of the boards are described below:

- Fund Management Board: responsible for managing administrated portfolios, which shall be carried out in accordance with strategies, sectoral and financial asset and private equity analyzes. The board is led by the "Management Officer"; designated directly in the Manager' articles of association, pursuant to art. 4, item III and paragraph 7 of CVM Resolution 21;

- Compliance, Risk, and PLD/FTP Board: responsible (i) for risk management of the portfolios administrated by the Manager and risk monitoring of financial assets, as described in the Manager's Risk Management and Liquidity Management Policy, (ii) for developing, approving, implementing, and monitoring rules, policies, routines, and internal controls adequate to the operational standards and legal and regulatory conduct, and (iii) for compliance with policies, procedures, and internal controls related to the prevention of money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction. The board is headed by the "Compliance, Risk, and PLD/FTP Officer"; designated directly in the Manager's articles of association, pursuant to art. 4, items IV and V and paragraph 7 of CVM Resolution 21, CVM Resolution 50 of August 31, 2021, and Law 9.613.

As applicable, local specialists and the global support team shall offer full support to the boards autonomously, performing tasks and operational procedures, as well as developing back office tasks essential to performance of the Manager's activities.

The organization chart of the organizational structure to be adopted by the Manager can be displayed as follows:



Without prejudice to the provisions of this Policy, as an entity that is part of the Lightrock Group, the Manager is subject to the provisions of Lightrock Group's policies and codes of conduct that establish Information Security guidelines and rules applicable to all employees of Lightrock Group and its affiliates .

1.2. GENERAL PROVISIONS

1.2.1. INITIAL PROVISIONS

This Information Security Policy is intended for the Manager's Collaborators and shall be observed by all.

The purpose of this Policy is to establish guidelines and responsibilities for information security management, according to the sensitivity of the data and information under the Manager's responsibility. Information security ("Information Security") is hereby characterized by the preservation of the following principles:

a) **Confidentiality:** is the guarantee that the information is accessible only by people with authorized access;

b) **Integrity:** is the guarantee that the information and processing methods shall be accurate, exact, complete, and up-to-date; and

c) **Availability:** it is the guarantee that authorized users obtain access to stored information and corresponding assets, whenever necessary.

In order to make Information Security management effective, the Manager's executive board coordinates the necessary actions for implementation of the Information Security management model and evaluates Information Security from time to time, as well as recommends corrective and preventive actions.

As responsible for this Information Security Policy, the Compliance, Risk, and PLD/FTP Officer or another Collaborator appointed by the latter, with the assistance of the Global support team, shall carry out the following activities:

a) Identification of specific Information Security needs and proposal of necessary implementations;

b) Setup the equipment, tools, and systems provided to Collaborators with all necessary controls to comply with the security requirements established by this Information Security Policy;

c) Manage and protect backup copies of programs and data related to critical and relevant processes for the Manager;

d) Management of the business continuity plan;

e) Generate the necessary information for the audit with a sufficient level of detail to track possible failures and fraud;

f) Implement integrity controls for information stored electronically so that it can be considered valid as evidence;

g) Implement, provide, and monitor the storage, processing, and transmission capacity necessary to ensure the security required by the business areas;

h) Promote the Collaborators' awareness regarding the importance of information security for the Manager's business; and

i) Analysis of information security incidents and recommendations for necessary corrections.

The Manager's Compliance, Risk, and PLD/FTP Officer shall verify compliance with the Information Security Policy and recommend the necessary corrective actions. Thus, the Compliance, Risk, and PLD/FTP Board shall have a navigation control solution on the World Wide Web websites, with a policy on access profiles and governance, through a configurable firewall, where it will be possible to have control of all accesses made by Collaborators and Officers of the Manager on the web. That is, it shall be possible (i) to carry out an analysis of information traffic by Officers and Collaborators and (ii) to block access to certain navigation channels (e.g. social networks and websites with inappropriate content), in order to assist verification by the Compliance, Risk, and PLD/FTP Board of any irregular accesses in noncompliance with this Information Security Policy.

Additionally, the access passwords of Officers and Collaborators to the Manager's systems shall expire every six (6) months, and the change thereof is mandatory.

This Information Security Policy shall be reviewed in the event of material changes in the activities, infrastructure, or operations of the Manager. However, a minimum revision shall take place every three (3) years in order to verify the possible need to produce an updated version, to be approved by the Manager's Compliance, Risk, and PLD/FTP Board.

1.2.2. POLICIES

This Information Security Policy shall be implemented at the Manager through specific and mandatory procedures for all Collaborators, irrespective of their hierarchical level or institutional function, as well as employment relationship or provision of services.

The following guidelines are part of the Manager's Information Security Policy:

a) **The information belongs to the organization:** All information generated, acquired, or processed by the Manager is its exclusive property. There shall be prior communication with the immediate management for the hard copies containing critical information of the Manager to be taken out of the institution;

b) **Business-oriented security:** Security actions shall be planned and applied in accordance with the risk assessment for the Manager's business. The availability, use, access, and protection of information and its resources shall always occur in order to preserve the continuity and competitiveness of the Manager's business;

c) **Ownership of information:** All information stored at the Manager's premises is considered the Manager's property, and it shall be used exclusively in its interest

and adequately protected, whatever the storage medium, against violation, alteration, destruction, unauthorized access, and undue disclosure. Those responsible for the storage, custody, and handling thereof shall be responsible for its integrity, use, or disclosure;

d) **Classification of information:** Each Collaborator shall have access to the information necessary for their work, observing the concepts of Confidentiality, Integrity, and Availability;

e) **Responsibility:** Each Collaborator is responsible for the security of the assets and information that are in their custody and for all acts performed with their access identification. Whatever its form, the identification shall be personal, non-transferable, and it shall clearly and indisputably allow their recognition;

f) **Least privilege:** Collaborators shall only have access to information assets that are essential for full development of their work;

g) **Security culture:** The content of this Information Security Policy and other standards shall be broadly disclosed at the Manager;

h) **Computing resources:** The computing resources made available by the Manager shall be used only for the development of activities related to the Manager's business; and

i) **Information Security Training:** Collaborators shall know and observe the organization's Information Security Policy. Whenever this Policy is reviewed and updated, an education and training program shall be carried out, whether in person or remotely, to ensure the dissemination of updated information, as well as to ensure knowledge and understanding of confidentiality and segregation policies and procedures in effect for information currently available, and awareness of the consequences of non-compliance with said rules and procedures.

1.3 CYBER SECURITY

1.3.1 OBJECTIVE

This chapter aims to define the guidelines to compose the Manager's cybersecurity program, which seeks to ensure the confidentiality, integrity, and availability of the data and information systems used.

1.3.2 RESPONSIBLE PERSON

The Compliance, Risk, and PLD/FTP Officer, with the support of local specialists and the global information technology team, is responsible for implementing the prevention and protection processes described in this policy and the respective treatment to be adopted regarding issues involving cybersecurity within the scope of the Manager. Any cybersecurity-related incident shall be immediately reported to the Compliance, Risk, and PLD/FTP Officer.

1.3.3 RELEVANT ASSETS

Within the Manager's scope of action, the relevant assets to be considered for analysis of internal and external risks and which require protection and prevention actions are:

- Data and Information: Confidential Information (as defined in the Compliance and Internal Controls Policy), including information regarding investors, clients, Collaborators, and the Manager itself, operations and assets invested by the securities portfolios managed by it and internal and external communications;
- Systems: information about the systems used by the Manager and the technologies developed internally and by third parties for functionality of the Manager's activities;
- Processes and Controls: internal processes and controls that are part of the routine of the Manager's business areas.

1.3.4 THREAT SCENARIOS

With regard specifically to cybersecurity, the Manager identified the following main threats, in accordance with ANBIMA's Cybersecurity Guide:

- Malware – software developed to corrupt computers and networks (such as: Viruses, Trojan Horses, Spyware, and Ransomware);

- Social engineering – manipulation methods to obtain confidential information (Pharming, Phishing, Vishing, Smishing, and Personal Access);

- DDoS attacks (distributed denial of services) and botnets: attacks aimed at denying or delaying access to the institution's services or systems;

- Invasions (advanced persistent threats): attacks carried out by sophisticated intruders using knowledge and tools to detect and exploit specific weaknesses in a technological environment.

1.3.5 PREVENTION AND PROTECTION ACTIONS

The Manager established the following group of action and prevention measures to mitigate the risks identified above, noting that each Collaborator is responsible for maintaining control and security of the information held in their custody in their respective equipment:

(i) Regarding the process of printing files used by Collaborators, it is expressly forbidden that the respective data circulate outside the Manager's premises, as they are sources of Confidential Information. This provision does not apply to cases in which the transport of documents is necessary for purposes of the Manager's operations, and the Collaborator shall be responsible for the safekeeping, good conservation and use thereof;

(ii) At the Manager's physical workstations, computers shall not be left in open sessions when the responsible Collaborator is absent;

(iii) Any disposal of information both digitally and physically shall be done in such a way that file recovery is impossible.

(iv) All passwords and logins, corporate e-mails, and internal systems of the Manager shall be known exclusively by the Collaborator and may be transferred, and shall not be disclosed to third parties.

1.3.6 RESPONSE PLAN

In any suspicion or case of risk to the Manager's relevant assets described above related to cybersecurity, the Compliance, Risk, and PLD/FTP Officer shall be immediately called to restore order in the information systems.

1.3.7 INTELLECTUAL PROPERTY

Any document or file produced, modified, adapted by Officers, Managers, or Collaborators, directly or indirectly related to the work carried out at the Manager, such as agreements, presentations to clients, emails, memos, and registered purchase and sale orders are the property of the Manager and shall not be used after the professional leaves the Manager.

1.4. FINAL PROVISIONS

1.4.1 CONSEQUENCES OF BREACH

The Manager is exempted any and all liability arising from improper, negligent, or reckless use of the resources and services granted to its Collaborators, and it reserves the right to analyze data and evidence to obtain evidence to be used in investigative processes, as well as take the appropriate legal measures.

Failure to comply with the policies and procedures established in this Information Security Policy shall result in the following measures, according to the understanding of the Compliance, Risk, and PLD/FTP Officer (or, if the Compliance, Risk, and PLD/FTP Officer is involved, any other Officer):

(i) dismissal of Collaborators involved in the non-compliance in question, including those who were aware of the non-compliance in question and failed to report it to their superiors; and/or

(ii) liability of the Collaborators involved in the non-compliance for any damages the Manager may suffer as a result of their conduct.

Imposition of the above penalties does not exempt, waive, or mitigate civil, administrative, and/or criminal liability for damages resulting from its intentional or faulty acts resulting from violation of the applicable law and the policies and procedures established in this Information Security Policy.