
COMPLIANCE AND INTERNAL CONTROLS POLICY

OF

LIGHTROCK GESTORA DE RECURSOS LTDA.

APRIL 17, 2023

1. COMPLIANCE AND INTERNAL CONTROLS 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 activity, in the asset manager category, pursuant to CVM Resolution No. 21 of February 25, 2021, as amended ("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 in which it engages, 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; (ii) securities trading policy; (iii) risk management and liquidity management policy; (iv) business plan; (v) information security policy; (vi) order division and sharing policy; (vii) this Compliance and Internal Controls Policy (as defined below); (viii) policy to prevent money laundering, terrorism financing, and financing of the proliferation of weapons of mass destruction ("PLD/FTP"); (ix) third-party contracting policy; and (x) private credit management policy (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 policy on rules, procedures, description of internal controls, segregation of activities, and confidentiality rules ("Compliance and Internal Controls Policy"), with the purpose of establishing general provisions on the Manager's internal compliance, it being understood that, represented by the Compliance, Risk, and PLD/FTP Officer, the Manager shall continuously monitor compliance with the Internal Policies provided for in this document by the Collaborators.

This policy aims to establish rules and procedures, as well as describe the compliance and internal controls program to be implemented and observed in the performance of the Manager's activities.

Upon receiving a copy of this Compliance and Internal Controls Policy, Collaborators shall sign an instrument of adhesion, in accordance with the form contained in Exhibit I hereto ("Exhibit I"), through which they will represent, without limitation, that: (i) they have received a copy of the Compliance and Internal Controls Policy; (ii) they have read and understood the entire content of the Compliance and Internal Controls Policy; (iii) they are aware of and agree with the terms and conditions of the Compliance and Internal Controls Policy, undertaking to fully observe the Manager's internal policies provided for in this Compliance and Internal Controls Policy ("Instrument of Adhesion").

Collaborators may also consult this Compliance and Internal Controls Policy at the Manager's electronic address: www.lightrock.com .

This Compliance and Internal Controls Policy shall be updated at least annually by the Manager's Compliance, Risk, and PLD/FTP Officer (as defined below), in order to contemplate any amendments to the laws, regulations, self-regulations, and applicable best practices. Whenever this Compliance and Internal Controls Policy is updated, the Collaborators shall receive a new copy of the updated Compliance and Internal Controls Policy (printed and scanned), and shall sign a new Instrument of Adhesion.

The Instruments 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 term of professional relationship with the Collaborator and for an additional term of at least five (5) years as from the Collaborator's termination date, for any reason.

In addition to reading this Compliance and Internal Controls 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 Compliance and Internal Controls 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 laws, regulations, self-regulations, and best market practices.

Organizational Structure of the Manager

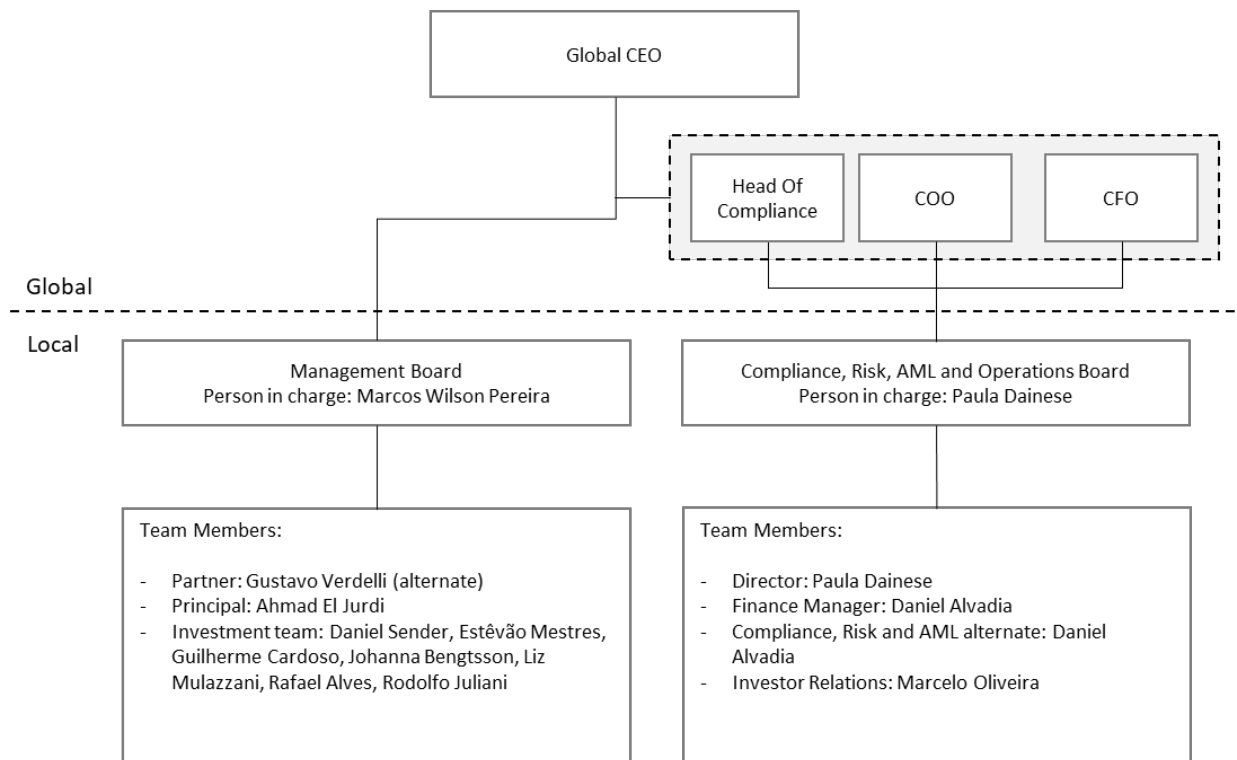
The Manager was organized to act in the securities portfolio management and its organizational structure is divided into two (2) distinct areas, namely: (i) fund management, and (ii) compliance, risk management, and PLD/FTP. The Manager establishes and develops mechanisms to guarantee the independent performance of all areas.

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

- Fund Management Board: responsible for managing administrated portfolios, which should be carried out in accordance with strategies, sectoral and financial asset analyzes, and private equity. The board is led by the “Management Officer”; designated directly in the Manager’s articles of association, pursuant to art. 4, item III and paragraph 7 of CVM Resolution 21; and
- 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 of 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 No. 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 the development 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 in policies and codes of conduct of the Lightrock Group that establish Compliance guidelines and rules applicable to all collaborators of the Lightrock Group and its affiliates.

Introduction of the Compliance and Internal Controls Policy

The Compliance, Risk, and PLD/FTP Officer shall be responsible, without limitation, for ensuring, through appropriate rules, procedures, and internal controls, permanent compliance with the applicable rules, policies, and regulations, in addition to monitoring policies on the prevention of and fight against money laundering and ensure the Manager's compliance with the applicable laws and regulations. This policy is also used to encourage the constant updating and training of Collaborators in order to maintain excellence in the provision of services to clients. It also serves to monitor possible operational errors, conflicts of interest, and ensure adherence to the Manager's other policies, all disclosed on the electronic address available in printed and scanned copy to all Collaborators.

The Manager's internal compliance shall involve the following activities:

- i. periodic inspection of routines, rules, and procedures provided for in this Internal Policy, in order to identify possible violations;

- ii. imposition of penalties to Collaborators who violate the Internal Policy, which may involve disciplinary actions, including warning, removal from the Manager's corporate structure, termination of the employment relationship, or termination of the services agreement or the contract that binds them to the Manager, as applicable, without prejudice to any applicable administrative and/or legal measures;
- iii. coordination of the Manager's interactions with its regulators and self-regulatory bodies, as well as coordination with other areas and departments to strengthen the Manager's general control environment;
- iv. request, whenever necessary, support from external consultants to analyze more complex issues involving the Manager's internal compliance; and
- v. periodic updating of this Internal Policy, in order to reflect amendments to the laws, regulations, self-regulations, and best market practices.

In case of conflict between the general provisions set forth in the Internal Policies and the specific provisions of this Compliance and Internal Controls Policy, the specific provisions of this Compliance and Internal Controls Policy shall prevail.

1.2. INFORMATION SECURITY POLICY

Portfolio administration and management activities involve access to Confidential Information owned by its clients. The Manager understands the seriousness and level of clients' trust in the Manager and, therefore, treats information security very seriously.

All of the Manager's files shall be stored on servers whose companies have an unblemished professional reputation in their respective areas of activity. All access to the systems used by Collaborators shall be protected by passwords and any physical documents containing Confidential Information about the assets of clients shall contain coding instead of full names.

Free access to the Manager's premises shall be restricted to Collaborators, and access to the Manager's premises by clients and technical advisors shall be limited to areas where securities portfolio management activities are not carried out (such as, for example, meeting rooms).

For purposes of this Compliance and Internal Controls Policy, the definition of "Confidential Information" encompasses any data, materials, information, documents, technical or commercial specifications, analyses, studies, and projections that are not public knowledge, obtained orally or in writing, in hard copy and/or electronic media, prepared or disclosed to

any Collaborators of the Manager, including, but not limited to, data from inactive, active, and/or prospective clients; business plans, investment and divestment plans; financial valuations; bank information; information about administrative proceedings, lawsuits, and/or arbitration proceedings processed under seal; memoranda of understanding; agreements; memos; reports; researches; spreadsheets; presentations, among other secret, confidential documents or documents without public access.

1.3. TRAINING AND CERTIFICATIONS

The Manager believes that the Collaborators' continuous learning raises the team's level of knowledge and adds value to the Manager. Therefore, the Manager shall encourage all those involved to seek to improve their knowledge.

This improvement can be done through internal and external training, external courses (undergraduate, graduate, specialization, and/or training) and/or certifications required by the applicable regulations.

Annual plans shall be developed for appropriate internal training related to the provisions of the Internal Policies, aimed at training and raising awareness of Collaborators in matters inherent in the activities of the Compliance, Risk, and PLD/FTP Board for greater adherence to issues related to information security, risk management, compliance, and internal controls.

The training shall be carried out on a date to be determined by the Manager, under the supervision of the Compliance, Risk, and PLD/FTP Officer, and the presence of all Collaborators is mandatory. Each Collaborator shall sign a declaration that he/she participated in the training.

1.4 CERTIFICATION POLICY

1.4.1 OBJECTIVE

In accordance with the provisions of the ANBIMA Certification Code ("Certification Code"), this chapter aims to establish the criteria for eligible professionals to be duly certified to work in the Manager's segments.

1.4.2 ELIGIBLE ACTIVITIES AND IDENTIFICATION CRITERIA

ANBIMA requests a certification program for professionals who will work in entities linked to their codes, considering the scope of each professional's work.

Considering the Manager's activity in the management of third-party funds, through equity investment funds, governed by CVM Instruction No. 578 of August 30, 2016, as amended, and investment funds governed by CVM Instruction No. 555 of December 17, 2014, as amended ("FIP" and "555 Funds", respectively), the following certificates are required:

- (i) CFG: applicable to the Manager's professionals who carry out the professional exercise of third-party fund management. It is not mandatory and is not a condition to work in any specific activity, but it is a prerequisite for CGA and/or CGE certification;
- (ii) CGE: applicable to the Manager's professionals who carry out the professional exercise of FIP third-party fund management, with investment authority/discretionary power;
- (iii) CGA: applicable to the Manager's professionals who carry out the professional activity of 555 Fund third-party fund management, with investment authority/discretionary power.

The Manager shall ensure that Collaborators who work in eligible activities participate in the procedure for updating their respective certifications, so that the certification obtained is duly updated within the terms established in the Certification Code.

1.4.3 IDENTIFICATION OF NEW COLLABORATORS

Any and all analysis of hiring, admission, or transfer of a Collaborator between areas shall be preceded by an analysis by the Fund Management Officer to confirm the need for certification in view of the investment decision authority/discretionary power the Collaborator shall exercise.

Once the Collaborator's need for certification has been verified, he/she shall prove his/her certification or exemption, if applicable, at the time of hiring, admission, or transfer.

1.4.4 ANBIMA DATABASE UPDATE

The identification of all certified Collaborators shall appear in the Anbima Database, considering that updates, pursuant to art. 12, paragraph 1, I of the Certification Code shall be carried out by the last business day of the month following the date of the event that caused the update, noting that the inclusion of self-employed investment agents, contracted third parties, and interns is optional, updates becoming mandatory if such information is included in the ANBIMA Database.

The Compliance, Risk, and PLD/FTP Officer shall check whether Collaborators who are leaving the Manager are indicated in the ANBIMA Database as eligible/certified professionals linked to the Manager.

1.4.5 MONITORING

Jointly, the Compliance, Risk, and PLD/FTP Officer and her team shall monitor and inspect the Collaborators on a quarterly basis to ensure that (i) Collaborators with investment authority/discretionary power are duly certified or in the process of certification, according to the Certification Code, and (ii) the Collaborators are duly identified in the ANBIMA Database.

Collaborators who do not hold the CGA or CGE, as applicable, or who do not prove exemption of such certificate granted by the Certification Board, pursuant to art. 16 of the Certification Code, shall be prevented from exercising authority/discretionary power to purchase and sell assets for the FIPs or for the 555 Funds, as applicable, without the prior approval of the Fund Management Officer.

Furthermore, during the verifications required, the Compliance, Risk, and PLD/FTP Officer shall request, upon verification of nonconformity of the functions performed by Collaborators because they are acting without the necessary certification or with expired certification, that the Collaborator immediately cease the duties involving authority/discretionary power to invest the assets comprising the FIPs' and the 555 Funds' portfolios, due to noncompliance with the provisions of the Certification Code, until such Collaborator is able to perform the respective duties again.

If professionals already certified, who have authority/discretionary power to invest in the assets comprising the FIPs' and the 555 Funds' portfolios, cease to be Collaborators of the Manager, they shall sign the documentation provided for in Exhibit II to this Compliance Policy called "Instrument of Withdrawal", proving their withdrawal from the Manager. The same procedure for signing Exhibit II shall immediately apply to non-certified professionals or professionals in the process of certification who are removed for any of the reasons mentioned above.

1.5. CONTINGENCY PLAN

Due to the nature of the fund management activities carried out by the Manager, the company is subject to extensive legislation, regulations, and self-regulations in the Brazilian market. In order to fully meet these requirements, as well as adapt its activities to the best market practices, the Manager shall adopt this policy that describes the Contingency Plans for Business Continuity ("PCCN"), under the direct responsibility of the Compliance, Risk, and PLD/FTP Officer.

The PCCN aims to ensure the continuity of the Manager's business in the event of acts of God or force majeure that may affect its physical or technological infrastructure ("Disruptive Event").

The PCCN is described below and shall be reviewed and updated annually by the Compliance, Risk, and PLD/FTP Officer, so that it is always up to date.

1.5.1 WORKPLACE AND COLLABORATORS

Upon occurrence of an event that makes it impossible for Collaborators to access the Manager's office, they shall return to their respective homes, in order to perform their duties from remote access to the Manager's network (using their credentials to release access) and await instructions from the Compliance, Risk, and PLD/FTP Officer. The communication shall be carried out by means of a telephone call, e-mail, or other means of communication authorized by the Compliance, Risk, and PLD/FTP Officer.

If the office remains closed for more than twenty-four (24) hours on a business day, Collaborators shall keep activities remotely, except in the event that the Compliance, Risk, and PLD/FTP Officer chooses to allocate the work team in a support location, to be defined by such Officer.

The Manager's technology system shall have a remote access option, allowing Collaborators to carry out their activities normally without being physically present at the company's premises, as per subitem 1.4.4.

1.5.2 COMMUNICATION

Additionally, as soon as possible, all clients shall be notified (by email, correspondence, or phone call) by the Manager about occurrence of the Disruptive Event, the alternative forms of contact, and deadlines for the Manager to solve the problem. The Compliance, Risk, and PLD/FTP Officer shall be responsible for carrying out this communication.

1.5.3 FILE PROTECTION

The Manager shall store files in the cloud with high storage capacity, restricted access controlled by the Compliance, Risk, and PLD/FTP Officer, with the assistance of Information Technology professionals. E-mails and files shall be hosted in an environment determined as a cloud (cloud computing).

1.5.4 REMOTE ACCESS TO THE MANAGER'S SYSTEMS

Collaborators may perform their duties from any computer with access to the world wide web. Remote access to the Manager's essential systems shall be available, with individual logins and

passwords for all Collaborators. Collaborators shall set up their private computers to have access to files on the Manager's systems. The professional e-mail can be accessed via the Internet by all Collaborators.

1.5.5 POWER OUTAGE - NO BREAKS

All access to the Manager's digital systems shall be carried out by means of desktop and/or mobile devices, with a minimum self-sufficiency of up to one (1) hour of operation without a power source. All Collaborators of the Manager shall be instructed to keep their mobile devices with full battery storage.

In the event of sudden and abrupt power outages, Collaborators shall reduce as much as possible the execution of activities that require electricity, simultaneously promoting the completion of necessary tasks and storage of documents in progress.

1.5.6 IMPLEMENTATION OF EMERGENCY PROCEDURES

The table below describes the events, procedures, and allocation of duties to be adopted in emergency cases:

List of Events		
Occurrence	Person in Charge	Procedure
Power outage	Compliance, Risk, and PLD/FTP Officer	Remote access or use of no-breaks.
Internet outage	Compliance, Risk, and PLD/FTP Officer	Remote access.
Building Access	Compliance, Risk, and PLD/FTP Officer	Remote access.
Fire	Compliance, Risk, and PLD/FTP Officer	Remote access.

1.6. COMPLIANCE SYSTEMS AND INSTRUMENTS USED

The Compliance, Risk, and PLD/FTP Officer shall establish, in the program, the procedures, parameters, obligations, and internal routines that shall be observed and monitored and creates specific reports and mechanisms for each obligation applicable to the Manager, which makes the service personalized, autonomous, and fully adapted to the Manager.

Finally, all Compliance reports, instruments of adhesion to this Compliance and Internal Controls Policy, spreadsheets, communications, communications with regulatory and self-regulatory bodies, among others, are stored on the Manager's own server, in the cloud (cloud computing), and copies in a folder with access restricted to members of the Compliance, Risk, and PLD/FTP area.

1.7. RULES AND PROCEDURES RELATED TO SEGREGATION OF ACTIVITIES

In view of the activities that make up the Manager's corporate purpose, pursuant to the provisions of its corporate documents, the Manager's activities and areas ("Areas of Expertise") are:

- (i) carrying out the securities portfolio management activity, in the capacity as an investment fund manager, pursuant to the provisions of the applicable regulations ("Third-Party Fund Management"), which shall be the responsibility of the Management Officer; and
- (ii) the provision of consulting services, including auditing, analysis, and support services to companies and other entities located abroad ("Consulting").

Please note that both Areas of Activity shall be carried out by the same Collaborators and that, pursuant to the provisions of the applicable regulations, the imposition of compulsory segregation is only and solely due between the area responsible for managing securities portfolios and the areas responsible for the intermediation and distribution of securities (other than own funds), which activity is not performed by the Manager.

Indeed, although there is no need to segregate activities, either by the literal text of the rule or by the broad concept of risk of unlawful acts, in fact the rule does not prohibit the existence of potential conflicts of interest, but requires that, in the event of potential conflicts of interest, market participants create mitigation mechanisms and that potential conflicts of interest are therefore duly referred to the CVM, investors, and companies operating in the market that may relate with the Manager for information purposes.

Therefore, there is currently no physical segregation between the Areas of Operation of the Manager, but only a segregation of its systems and access folders in the directory, and all regulatory obligations are being duly met.

All Collaborators shall observe the rules and segregations established in this Compliance and Internal Controls Policy and grant strictest confidential treatment to the information to which they may have access due to exercise of their activities. For that purpose, each Collaborator,

upon signing the Instrument of Adhesion, expressly certifies to agree to the rules established in the Internal Policies and, by signing a non-disclosure agreement, refrains from disclosing confidential information to which he/she may have access.

In order to deal with a potential or effective conflict of interest between the activities of each Area of Expertise, the following measures shall be taken, without prejudice to the Manager's continuous duty of trust, and continuous performance in good faith:

- (i) the Manager shall include in the documentation of the investment funds it manages, notably in the funds' bylaws, in order to give wide and full disclosure of information to shareholders, express wording regarding the possibility of acting as a consultant for the target companies or those in which the funds invest;
- (ii) if the managed funds wish to make investments in companies in which the Manager already acts as a consultant, all necessary measures shall be taken to make the investment possible without any regulatory noncompliance, and it may even request the fund manager to call a shareholders' meeting for resolution on the matter, if necessary; and
- (iii) when it comes to contracting consulting services to work with companies invested in by the funds managed by the applicant, the latter shall previously take all necessary measures to enable the contracting without any regulatory non-compliance, requesting the fund manager to call a shareholders' meeting for resolution on the matter, if necessary. With that, the Manager emphasizes that all regulatory obligations are being duly met because: (i) it has manuals with clear and objective information, and adequate controls; and (ii) it has a training policy for all its Collaborators, in order to (a) ensure the proper use of facilities, equipment, and common information, (b) preserve confidential information and allow the identification of people who have access thereto, if applicable, and (c) restrict access to files and allow identification of persons who have access to confidential information.

Also, considering that it is difficult for a policy to foresee all possible situations, it is necessary to use common sense and discernment when facing situations not contemplated in this Compliance and Internal Controls Policy. When in doubt, the Officers and Collaborators of the Manager should seek guidance from the Compliance, Risk, and PLD/FTP Officer whenever necessary.

EXHIBIT I. INSTRUMENT OF ADHESION

INSTRUMENT OF ADHESION TO THE INTERNAL POLICIES OF LIGHTROCK GESTORA DE RECURSOS LTDA.

I, [insert full name of the Collaborator], [nationality, marital status, occupation], bearer of identity card RG No. [complete], enrolled in the Individual Taxpayer's Register of the Ministry of Economy (CPF/ME) under No. [complete], resident and domiciled at [complete], in the capacity as [inform Collaborator's position] of

LIGHTROCK GESTORA DE RECURSOS LTDA., a limited liability business company with its principal place of business in the municipality of São Paulo, state of São Paulo, at Rua Joaquim Floriano, No. 1120, suite 122, Postal Code (CEP) 04.534-004, enrolled with the National Corporate Taxpayers' Register of the Ministry of Economy ("CNPJ/ME") under No. 27.927.837/0001-37 ("Manager"), irrevocably and irreversibly represent that:

(i) I received, on the date hereof, the updated version of the following internal policies of Lightrock Gestora de Recursos Ltda.: (i) code of ethics; (ii) securities trading policy; (iii) risk management and liquidity management policy; (iv) business plan; (v) information security policy; (vi) order division and sharing policy; (vii) this Compliance and Internal Controls Policy (as defined below); (viii) policy on the prevention of money laundering and terrorism financing and the financing of the proliferation of weapons of mass destruction; (ix) third-party contracting policy; and (x) private credit management policy ("Internal Policies");

(ii) I read the Internal Policies in full, clarified any doubts, and understood the content thereof;

(iii) I express my unrestricted adhesion to the Internal Policies, agreeing to comply and ensure compliance with all their provisions;

(iv) I am aware that noncompliance with the provisions of the Internal Policies represents a serious breach in the performance of my duties at Lightrock, which may lead, in a manner already recognized by me as justified, to disciplinary actions, including warnings, removal from Lightrock's shareholding structure, termination of the employment relationship or termination of the services agreement or of the agreement that binds me to Lightrock, as applicable;

(v) I am aware that failure to comply with the provisions of the Internal Policies may subject me to administrative, civil, and criminal liability, as applicable;

(vi) I am fully aware that the Internal Policies are only intended to complement the laws, regulations, and self-regulation rules applicable within the scope of my duties at Lightrock (“Applicable Laws”) and do not prevail over the Applicable Laws, which shall be observed and complied with by me;

(vii) the Internal Policies shall be construed jointly and systematically with each other, and the annulment or invalidity of any provision of the Internal Policies does not imply annulment or invalidity of the other provisions of the Internal Policies, which shall remain in full force for the purposes for which they have been designed;

(viii) on the date of signature of this Instrument of Adhesion, there are no situations and/or I am not aware of any situations that could be classified as violations or conflicts of interest in relation to or in accordance with the Internal Policies;

(ix) on the date of signature of this Instrument of Adhesion, my personal investments neither breach nor infringe, in any way, the policy on the trading in securities and personal investments contained in the Internal Policies;

(x) I agree to report any actual or potential situation that may cause any representation made by me under this Instrument of Adhesion to become false, incorrect, or incomplete or which may in any way pose a risk to Lightrock ; and

(xi) I agree to observe and comply with the secrecy and confidentiality obligations assumed in the Internal Policies, especially in the chapter related to the confidentiality of Confidential Information, for a minimum period of ten (10) years as from the date of my effective dismissal or termination of my relationship with Lightrock.

Sao Paulo, **[Date]**

[Collaborator’s full name and signature]

EXHIBIT II
INSTRUMENT OF WITHDRAWAL

By means of this instrument, I, _____, enrolled with the Individual Taxpayer's Register of the Ministry of Economy (CPF/ME) under number _____, represent for all due purposes that, as of the date hereof, I withdraw from the third-party fund management activities of **LIGHTROCK GESTORA DE RECURSOS LTDA.**, enrolled with the National Corporate Taxpayers' Register (CNPJ) under No. 27.927.837/0001-37 ("Manager") for an indefinite period:

[] until I am certified by the CGA, in the case of the management of third-party funds with authority/discretionary power to invest in private equity investment funds, governed by CVM Instruction No. 578 of August 30, 2016, as amended;

[] until I am certified by the CGE, in the case of the third-party fund management activity with authority/discretionary power to invest in investment funds, governed by CVM Instruction No. 555 of December 17, 2014, as amended;

[] until the Certification Board, pursuant to Art. 16 of the Certification Code, grants me exemption from obtaining the CGA;

[] until the Certification Board, pursuant to Art. 16 of the Certification Code, grants me exemption from obtaining the CGE; or

[] considering that I am no longer a Collaborator of the Manager;

[•], [•] [•], [•].

[COLLABORATOR]

LIGHTROCK GESTORA DE RECURSOS LTDA.

Witnesses:

1. _____

Name:

Taxpayer Card (CPF):

pgi/336717.doc

05/25/23

2. _____

Name:

Taxpayer Card (CPF):