VBI REAL ESTATE

Manual of Rules, Procedures **and Internal Controls**

Escaneie o QR code com a camera do seu cellular e acesse as opções

July **2021**

CONTENTS

1. DEFINITIONS

The terms used in this document starting in capital letters have the meanings shown below.

"ABVCAP"	Means the Brazilian Association of Private Equity and Venture Capital.
"ANBIMA"	Means the Brazilian Financial and Capital Markets Association.
"ANBIMA Code"	Means the ANBIMA Code of Regulation and Best Practices for Managing Third-Party Resources.
"Associates"	Means the partners, officers, employees, interns, apprentice minors of VBI and service providers assigned to VBI.
"CVM"	Means the Brazilian Securities Exchange Commission.
"CVM Directive no. 558"	Means CVM Directive no. 558, of March 26, 2015, as changed.
"Department of Internal Controls"	Means VBI's Internal Controls and Risk Management area.
"Manual"	Means this Manual of Rules, Procedures, and Internal Controls.
"Policies"	Means the policies referred to in Item 2.1 below.
"Annual Adherence Report"	Means the compliance test performed annual, as referred to in Item 11 below.
"VBI"	Means VBI Real Estate Gestão de Carteiras Ltda. And/or, when the context allows, its subsidiaries.

2. OBJECTIVE

In the course of its business activities, VBI is subject to laws that govern the operation of the Brazilian capitals market, especially the regulations issued by the CVM, which currently governs the activity of portfolio management under its CVM Directive no. 558.

The purpose of this Manual is to define rules, procedures, and internal controls to be followed as parameters in VBI's business activities as a manager and consultant. These rules, procedures, and internal controls are adopted to always comply with applicable laws and regulations, the highest ethical and professional standards, and the forms of investment and the securities portfolio management activity by VBI and its Associates.

VBI has its own procedures that involve systems and internal controls necessary to follow, monitor, and assess internal policies and codes, rules issued by the CVM, the regulations issued by ANBIMA, especially the ANBIMA Code, the guidelines issued by ABVCAP, and applicable laws.

The content of this Manual is designed to ensure all applicable regulations, policies, and rules are complied with and to disseminate a culture of controls to ensure the compliance of rules defined by the regulatory and self-regulatory authorities. This Manual is not intended to comprehensively address all applicable regulations to VBI's business activities.

2.1. POLICIES

In addition to the policies attached to this Manual, as shown in Item 12 below, VBI also adopts the following codes and policies, which must be complied with by all its Associates and which are available on the VBI network, at "VBIREALESTATE/COMPLIANCE/POLÍTICAS", in the Compliasset System and on VBI's webpage on the internet:

(i) Code of Ethics and Conduct;
(ii) Risk Management Policy;
(iii) Order Apportionment and Division Policy;
(iv) Vote Policy;
(v) Personal Investments Policy;
(vi) Pricing Manual;
(vii) Private Credit Assets Acquisition and Monitoring Policy;
(viii) Real-Estate Assets Acquisition and Monitoring Policy;
(ix) Third Party Selection and Hiring Policy on behalf of the Funds;
(x) Preventing Money Laundering and Fighting Terrorism Financing Policy; and
(xi) Certification Policy.

3. SCOPE

The guidance contained in this Manual and its Exhibits should be followed by all VBI Associates, regardless of their hierarchical level and duration of the rendering of the services.

All Associates must adopt and comply with the guidelines and controls contained in this Manual and its Exhibits, ensuring that all ethical and legal rules are followed by all those with whom they maintain professional relations, immediately reporting any violations to the Compliance Committee, as shown in Item 14 below.

4. VBI CORPORATE PROFILE

VBI is an asset manager registered at the CVM under the "asset manager" category. VBI provides portfolio management services to local investment funds and consulting services to offshore investment vehicles, with a focus on the Brazilian real-estate industry and its related assets.

The main areas of resource allocation in the Brazilian capital markets and real-estate industry are the following:

(i) Residential projects;
(ii) Student housing projects;
(iii) Land subdivision projects;

(iv) Industrial logistics projects;
(v) Retail and shopping mall projects;
(vi) Office tower projects; and
(vii) Structured credit and financial instruments for assets related to the real-estate industry.

5. VBI PARTNERS

VBI's Partners are responsible, in a collegiate manner, for the following:

(i) Review proposals to change VBI's internal controls and reports forwarded by the Internal Controls Committee, which list all occurrences monitored during the quarter in question;
(ii) Approve VBI policies and codes, including those the Compliance Committee recommends being implemented or updated; and
(iii) Ensure the effectiveness of compliance risk management.

6. DIRECTOR OF INTERNAL CONTROLS AND COMPLIANCE

The Director of Internal Controls and Compliance is responsible for VBI's internal controls and compliance; he/she is responsible for:

(i) Helping the VBI's Partners ensure the effectiveness of VBI's internal controls and compliance processes, effectively managing these activities on a day-to-day basis;

(ii) Monitoring the activities of the Compliance Committee and the Internal Controls and Risk Management Committee, ensuring their good operation and that all decisions taken are recorded in meeting minutes;

(iii) Designating the secretary for the meetings of the Compliance Committee and the Internal Controls and Risk Management Committee; and

(iv) Monitoring and applying the necessary controls and procedures to comply with applicable regulations.

The Director of Internal Controls and Compliance reports to VBI's Partners and is free to question practices and procedures adopted in their operations and activities; the Director of Internal Controls and Compliance must adopt steps that prohibit or mitigate the effects in such operations and activities that may be considered improper, incorrect, and/or unapplicable.

7. COMPLIANCE COMMITTEE

7.1. COMPOSITION AND GUESTS

The Compliance Committee consists of the following members: (i) Director of Internal Controls and Compliance; (ii) Director of Risk Management; (iii) Financial Director; (v) founding partners of VBI. Other VBI Associates or external advisers may be invited to provide an opinion before the Compliance Committee, as well as to attend meetings and discuss matters dealt with in such meetings, but they will not be entitled to vote.

7.2. PURPOSE

Strengthen VBI's compliance culture, in order to identify, guarantee, and control the proper assessment of risks, of VBI performance, of adherence to internal controls, of the compliance with existing rules, policies, and regulations, including policies, codes, and instructions issued by VBI, ANBIMA, ABVCAP, and the CVM, all in accordance with parameters, methods, and standards defined internally and required by regulatory authorities.

The Compliance Committee will test adhesion to controls and to applicable laws, rules, and regulations. It is a specific activity of monitoring and encouraging everyone's involvement.

7.3. DUTIES

(i) Guide the implementation of VBI's internal control structures, which cover well-documented records, which clearly identify the responsibilities and authorizations described, as applicable;

(ii) Review and suggest creating new controls and improvements in those deemed deficient and monitor corrections of any deficiencies identified;

(iii) Follow the development of activities designed to define new rules, making sure they clearly define the responsibilities of each area and the points of controls of the risks;

(iv) Intermediate the relationship between areas resulting from divergencies to establish conformity;

(v) Guide the proper segregation of functions and separate responsibilities to avoid conflicts of interest and highlight points of control;

(vi) Permanently monitor compliance with policies, rules, procedures, and the law regulating VBI's businesses, helping implement them and ensuring the image of the organization is preserved in the market in general;

(vii) Act as a liaison between VBI and authorities such as the CVM, ANBIMA, and ABVCAP and approve or direct any non -routine interactions with public authorities;

(viii) Control and monitor the securing, maintenance, and renewal of legal permits, registrations, and certifications necessary before the CVM, ANBIMA, ABVCAP, and other authorities;

(ix) Define actions in case of reports, complaints, or information related to non-compliance of Policies and other internal rules or obligations included in the rules or documents entered;

(x) Assess any situations of non-conformity identified and define plans of action, in addition to penalties and punishments for violations of the Policies and other internal rules by Associates, as applicable;

(xi) Follow environmental liabilities or contingencies identified in assets owned by VBI companies;

(xii) Review the effectiveness and compliance of internal Policies and processes;

(xiii) Review and approve transactions or contracts that involve potential conflicts of interest in order to mitigate or resolve such conflicts;

(xiv) Approve transactions or contracts that involve regulatory or reputational risks which have been red-flagged;

(xv) Advise and follow the work of VBI's Internal Controls and Risk Management Committee; and

(xii) Report directly to the Partners.

7.4. REQUIRED QUORUM

Before a Compliance Committee meeting starts, it will be necessary to have in attendance most of its members, and to have the mandatory presence of the Director of Internal Controls and Compliance, or an alternate member appointed by this Director. The decisions will be approved by affirmative votes of the majority of those attending the meeting.

7.5. FREQUENCY OF THE MEETINGS

The Compliance Committee must meet at any time as summoned by any of its members, as needed, including under special circumstances, such as violations of VBI's Policies or other internal rules and/or changes in law impacting VBI's business activities, observing the minimum frequency of meetings that may be required by the applicable regulation or self-regulation

7.6. FORMALIZATION OF THE MEETINGS

The meetings will have formal minutes that will record all decisions taken. The minutes process includes writing, reviewing, and signing the minutes by the members of the Compliance Committee; the material produced is filed on a monthly basis. VBI will keep these documents on file for at least five years.

8. INTERNAL CONTROLS AND RISK MANAGEMENT COMMITTEE

8.1. COMPOSITION AND GUESTS

The Internal Controls and Risk Management Committee has the following members: (i) Financial Manager; (ii) Legal Manager; (iii) Compliance Manager; (iv) IT Manager; (v) Fund Administration Manager; (vi) Human Resources Manager; (vii) Risk Management Director and (viii) Internal Controls Manager.

Other VBI Associates or external advisers may be invited to provide an opinion before the Internal Controls and Risk Management Committee, as well as to attend meetings and discuss matters dealt with in such meetings, but they will not be entitled to vote.

8.2. Purpose

The activities performed by the Internal Controls and Risk Management Committee are designed to monitor and review compliance with the law, investment fund regulations, and other contracts, as well as to verify compliance with VBI's internal rules. This committee evaluates the effectiveness and

compliance of VBI Associates with the provisions of this Manual, its Exhibits, the VBI Code of Ethics and Conduct and support the work of the Compliance Committee.

8.3. DUTIES

(i) Monitor and implement guidelines decided by the Compliance Committee;

(ii) Assess whether recommendations for improvements to the internal controls have been properly implemented by Associates;

(iii) Certify whether the procedures comply with applicable rules, regulations, and laws;

(iv) Follow policies, procedures, responsibilities, and definitions applying to the mapped risk management structure;

(v) Review and suggest updates for VBI's policies and codes at least once a year and as necessary;

(vi) Review the reports prepared by regulatory authorities and internal and external audits regarding deficiencies of internal controls and the necessary steps to be taken by the areas involved;

(xvi) Make any recommendations deemed appropriate;

(xvii) Promote a culture of internal controls in all of VBI's business activities;

(xviii) Work to ensure actual physical segregation of VBI's activities, as recommended under applicable law;

(xix) Inform and report directly to the Compliance Committee any situations of non-conformity to the applicable rules and Policies and other internal rules of which they have identified; and

(xx) Follow the provisions of the VBI Risk Management Policy.

8.3.1. SPECIFIC ROLES

Each member of the Internal Controls and Risk Management Committee will have individual responsibilities in performing internal control activities based on the position held by such individual. The individual responsibilities will be the following and their accomplishment must be reported to the Internal Controls and Risk Management Committee or to the Compliance Committee:

(i) Financial Manager

(a) Prepare the payment management report – monitor the risk of misdirection or fraud involving payments;

(b) Monitor suspicious financial transactions

(c) Carry out routine obligations with regulatory and self-regulatory authorities

(ii) Legal and Compliance Manager

(a) Manage the compliance channel;

(b) Formalize the meeting minutes; and

(c) Hold audits.

(iii) IT Manager

(a) Prepare function segregation report; and

(b) Assist the Internal Controls and Risk Management Committee in the management of the Contingency and Business Continuity Plan, in accordance with the terms set forth therein;

(iv) Fund Administration Manager

(a) Prepare the market risk reports; and
(b) Send reports to the administrators of the funds managed by VBI.

8.4. REQUIRED QUORUM

Before an Internal Controls and Risk Management Committee meeting starts, it will be necessary to have in attendance most of its members. The decisions will be approved by affirmative votes of the majority of those attending the meeting.

8.5. FREQUENCY OF THE MEETINGS

The Internal Controls and Risk Management Committee must meet as necessary, as summoned by any of its members. Including, without limitation, when during atypical market behavior, as a result of the announcement of new assumptions and parameters and/or changes in law that cause loss of price references, observing the minimum frequency of meetings that may be required by the applicable regulation or self-regulation.

8.6. FORMALIZATION OF THE MEETINGS

The meetings will have formal minutes that will record all decisions taken. The minutes process includes writing, reviewing, and signing the minutes by the members of the Internal Controls and Risk Management Committee; the material produced is filed on a monthly basis. VBI will keep these documents on file for at least five years.

9. TERM AND COMMUNICATION

This Manual and its Exhibits will become effective on the date they are published and will remain in effect for an undetermined term.

This Manual and its Exhibits revoke and replace all prior versions and any other prior provisions in any other documents contrary to the provisions in this Manual and its Exhibits regarding this subject matter.

This Manual and its Exhibits will be reviewed as necessary at least once every two years by the Internal Controls and Risk Management Committee and anytime it is appropriate or required under

superseding law or regulations. The recommendations for updating this Manual will be submitted to the VBI partners for approval.

9.1. COMMUNICATION

This Manual and its Exhibits as well as any changes will be made available or are available in the VBI network (under "VBIREALESTATE/COMPLIANCE/POLÍTICAS"), in the Compliasset System or on the VBI page on the internet and communicated to all Associates of VBI as of the date they become effective.

VBI will present this Manula to ANDIMA in the ways this authority determines as of the date the Plan becomes effective and, if there are any changes, within fifteen (15) calendar days after such change, pursuant to Article 86 of the ANBIMA Code of Regulation and Best Practices for Managing Third-Party Resources, or lesser time to determined by ANDIMA.

VBI will provide copies of this Manual to all other supervisory authorities (including but not limited to CVM and ABVCAP, as applicable) whenever asked, in accordance with applicable law and regulations.

10. COMMUNICATION AND TRAINING

10.1. COMMUNICATION TO THE REGULATORY AND SELF-REGULATORY AUTHORITIES

VBI will always strive to comply with all requirements for reporting obligations and legal information to regulatory authorities.

Any nonconformity regarding issues of personal and professional conduct must be submitted to the VBI Compliance Committee for review and decision on the steps to be taken.

The Director of Internal Controls and Compliance must inform applicable oversight, regulatory, and self-regulatory authorities (including but not limited to CVM, ANBIMA, and ABVCAP, as applicable) anytime he/she, in the exercise of their duties, identifies an occurrence or signs of violation of any law these authorities enforce, within ten (10) working days of the occurrence or identification, or lesser time defined under other VBI policies or law or regulations in effect at the time of such facts.

10.2. PROFESSIONAL TRAINING AND EDUCATION

When joining the company, all VBI Associates will receive training on VBI's Policies and on this Manual and its Exhibits.

All Associates will undergo mandatory training at least every two years or as necessary as a result of changes in law or of material fact; this training will be coordinated by the Internal Controls Manager and will communicate updates on the Policies and this Manual, and reinforce in the team the understanding and the need to observe the rules specified above.

Each training will be recorded in the minutes of the Compliance Committee and will include an attendance sheet, which will be filed in a digital folder related to this matter; the Associate attendance will be recorded in a list attached to the minutes of such meeting.

VBI will provide the necessary education for its Associates to permanently remain technically and professionally trained to properly perform their corporate tasks.

11. ANNUAL ADHERENCE REPORT

To verify internal controls, their effectiveness and their consistency with the nature, complexity, and risks of VBI's operations, annual adherence tests will be applied, which will be formalized through the Annual Adherence Report.

The Annual Adherence Report will contain at least the information required under Article 22 of CVM Directive no. 558, as shown in the sample reproduced in Exhibit II-A of this Manual, always considering the guidance contained in Exhibit II-B, which will be available for consultation by the CVM at the offices of VBI.

The Annual Adherence Report is the responsibility of the Director of Internal Controls and Compliance. Once it is ratified by the Compliance Committee, it will be forwarded to the Board and to VBI's partners once a year by the last business day of April of each year, covering information for the prior calendar year.

12. EXHIBITS

The following documents are annexes to this Manual:

(i) **Exhibit I:** Statement of Commitment, referred to in Section 13 of this Manual;

(ii) **Exhibit II:** Sample of Annual Report

(iii) **Exhibit III:** Information Security Policy;

(iv) **Exhibit IV:** Contingency and Business Continuity Plan; and

(v) **Exhibit V:** Segregation of Activities Policy.

13. STATEMENT OF COMMITMENT

Each VBI Associate will receive an individual Statement of Commitment under which they will adhere to the entire content of this Manual and its Exhibits, as well as any later changes. This Statement of Commitment, whose sample is reproduced in Exhibit I of this Manual, must be signed by the Associate and turned in to the Personnel Department when the Associate is hired.

This Manual is part of the rules that guide the work relationship of VBI Associates, who by signing the Statement of Commitment will agree with the rules determined in the Manual.

Non-compliance with any of the rules listed hereunder and those included in the individual employment contract and other VBI verbal or written rules will be deemed a breach of contract and will subject such an Associate to applicable penalties.

To the extent allowed under the law, VBI will not be responsible before any third parties for Associates who have violated the law or committed violations in the performance of their duties. In case VBI is penalized or has a loss of any nature as a result of the actions of its Associates, VBI may exercise its rights of redress or indemnity against the parties responsible.

14. QUESTIONS, GUIDANCE, AND COMMUNICATION OF INCIDENTS

Regarding this Manual and its Exhibits, any request involving clarification or guidance by the Compliance Committee must be emailed to compliance@vbirealestate.com or through the Compliance Channel of the Compliasset System.

All Associates must report to the Compliance Committee, using the above email address, any suspected cases of illegal activities, bad faith conduct, and violations to internal rules, policies and procedures; any such reports will be treated confidentially.

15. Revision History

Below is a table indicating the history of revisions to this Policy:

Version	Approval Date
1	July 13th ,2021.

EXHIBIT I – STATEMENT OF COMMITMENT

Name:		
Area:	Position:	
Personal ID no.:	Personal ID type:	CPF/MF:

I hereby declare I have fully read the Manual of Rules, Procedures, and Internal Controls and its Exhibits (the "Manual") of VBI Real Estate Gestão de Carteiras Ltda. ("VBI"), applicable to VBI and/or when the context allows, its subsidiary companies, and I am aware of its contents, which are directly associated with the performance of my duties.

Pursuant to this Statement, I promise to:

(i) Adopt and follow the guidelines stated in the Manual;

(ii) Immediately communicate to the Compliance Committee any violation of the Manual I may become aware of, regardless of any individual judgement, materiality, or relevance of the violation.

I am aware and agree that my physical, logical, biometric voice and image accesses can be monitored.

I hereby unconditionally agree to follow and comply with any new guidelines and rules that might be incorporated into the Manual without having to sign a new statement of commitment; I am also aware that in case of negligence or carelessness in applying the Manual of the disciplinary responsibility applying on such non-compliance.

[location], [date]

_____

Signature of the Associate

EXHIBIT II-A – SAMPLE OF ANNUAL ADHERENCE REPORT

Dear
Partners and Directors of
VBI Real Estate Gestão de Carteiras Ltda.

Ref.: **Annual Adherence Report – CVM Directive no. 558, of March 26, 2015, as changed ("CVM Directive no. 558")**

Dear Sirs/Madams,

In compliance with the provisions of Article 22 of CVM Directive no. 558, we hereby present you the report on the activities of VBI Real Estate Gestão de Carteiras Ltda. ("VBI") in [year] (the "Report").

In accordance with CVM Directive no. 558, this Report contains the following:

The findings of the examinations carried out;

Recommendations regarding any deficiencies observed, as well as a schedule for addressing them, as applicable; and

Statement of the director responsible for administering the securities portfolios or, as applicable, the director in charge of risk management, regarding any deficiencies observed in prior audits and the steps planned based on a specific schedule or actually carried out to address such deficiencies.

This Report will be available to the CVM at the offices of VBI for later referral, checks or audits by CVM.

Accordingly, we describe below the elements of this Report.

Findings of the examinations carried out (CVM Directive no. 558, Article 22, I)

(list in details according to area/occurrence, with all pertinent information, including the dates the occurrence was observed and its nature.

Statements of the director responsible for complying with the internal rules, policies, procedures, and controls on Prior Checks and the Respective Steps Planned (CVM Directive no. 558, Article 22, II)

(list in details according to area/occurrence, with all pertinent information, including the estimated dates of follow-up and the conclusion of the solutions)

Statements of the director responsible [for administering the portfolio and complying with the internal rules, policies, procedures, and controls]

(list in details)

This being all for the time being, we remain at your disposal to provide any clarifications you deem necessary.

Sincerely,

Director of Internal Controls and Compliance

Director responsible for administering the portfolios

EXHIBIT II-B – GENERAL GUIDANCE ON THE TECHNICAL CONTENT OF THE ADHERENCE TEST

VBI's Compliance Committee must design active controls and records over the year to compose the Annual Adherence Report described in Exhibit II-A of the Manual, at least regarding the matters listed below.

Such matters must, over the year, be addressed and monitored by the Compliance Committee and, as necessary, be object of close follow-up by high management (partners and directors) of VBI.

Such control must rely on specific worksheets that will act as tools of compliance and control of operational risk.

Controlling and recording over the year the events listed below are part of the core obligations of the Compliance Committee.

I. **Findings of the examinations carried out (CVM Directive no. 558, Article 22, I)**

(list in details according to area/occurrence, with all pertinent information, including the dates the occurrence was observed and its nature.

The control worksheet must include at least the following events taking place over the year, as well as their consequences, losses, and remedial steps taken:

(i) Operational errors involving transactions of the portfolios and funds managed;

(ii) Errors pertaining to financial transactions of clients;

(iii) Errors in the payment of compensation to dealers or brokers of funds paid to brokers or any service providers;

(iv) Failure to comply with any procedure provided for in the Third Party Selection and Hiring Policy on behalf of Investment Funds;

(v) Nonalignment of portfolios, communication with the administrator, and realignment;

(vi) Any other violation of legal rules observed;

(vii) Fund liquidity events;

(viii) Operational errors relative to the technological infrastructure and correction plan implemented;

(ix) Any instances the Contingency and Business Continuity Plan was triggered;

(x) Supplier errors;

(xi) Errors involving any internal policies, manuals, or codes or legal regulations and the rectification plan implemented;

(xii) Expressive changes in parameters of fund liquidity;

(xiii) Events related to risk management especially those involving the risk of credit and liquidity;

(xiv) Communications or any other alerts and communications received from regulatory authorities, or legal, arbitration, or administrative proceedings involving the CVM, ANBIMA, or ABVCAP, or other applicable regulatory authorities;

(xv) Non-compliance of certification obligations;

(xvi) Any breaches of contract;

(xvii) Any violations of the duty of contract confidentiality; and

(xviii) Any other events considered relevant by the Compliance Committee and which have placed at risk the company, its Associates, clients, portfolios under management, or good market practices.

EXHIBIT III – INFORMATION SECURITY POLICY

1. DEFINITIONS

The terms used in this document starting in capital letters have the meanings shown below. If not shown here, they will have the meanings attributed to them under VBI's Rules, Procedures, and Internal Controls Manual.

"Commission"	Means VBI's Internal Controls and Risk Management Commission.
"IT Manager"	Means the Information Technology Manager.
"Confidential Information"	This is information the property of or relative to VBI or its business activities, Associates, partners, clients, service contractors, providers, and any other third parties and which information is not in the public domain, especially information that: (i) Identifies personal, property, or strategic data; (ii) Is covered under a confidentiality agreement entered with third parties; (iii) Identifies strategic actions of the company's businesses, of its clients, or of its portfolios under management, whose disclosure may harm the management of businesses, clients, or portfolios managed by VBI or reduce its competitive advantage; (iv) Consists of technical, legal, or financial information, written or electronically filed and which pertain to VBI's business activities and which is duly identified as being confidential, represents intellectual or industrial property, and which is not otherwise available to the public at large; (v) Is so considered under a court order, legal provision, and/or regulation; (vi) The Associate uses for authenticating their identity (access passwords or name badges) and which is personal and non-transferrable; and (vii) Is so considered under order of VBI's Board.
"Manual"	Means VBI's Manual of Rules, Procedures, and Internal Controls.
"Policy"	Means this Information Security Policy.

2. OBJECTIVE

Information is increasingly important within contemporary society. For this reason VBI developed this Policy to adjust issues of strategic interest for the company.

This Policy describes proper conducts for handling, controlling, and protecting information, emphasizing forbiddance of improper disclosure and unauthorized access, whether wrongfully or willfully, in order to minimize the risks of robbery, fraud, spying, loss, accidents, and other threats.

The Policy has a broad understanding and its scope includes information transmitted in any form, written, visual or verbal, under formal and informal circumstances. Regardless of the form of disclosure, information security as described above must always be followed.

3. SCOPE

The contents of this document must be known to and obeyed by all VBI partners and Associates. Each Associate must comply with its guidelines and rules and make sure they are complied with by third parties (including visitors and service providers) who, under their responsibility, have access to VBI's facilities or systems.

4. PRINCIPLES AND GUIDELINES

The conduct of Associates regarding information security must always rely on the principles and guidelines listed below.

4.1 PRINCIPLES

(i) **Confidentiality:** Only personnel duly authorized by the company can have access to information maintained by VBI;

(ii) **Availability:** Authorized personnel must have access to information whenever necessary; and

(iii) **Integrity:** Information must be kept in its original state in order to protect during storage or transmission from any undue changes, whether accidental or intentional.

4.2 GUIDELINES

(i) Only legal, ethical, and administratively permitted activities can be performed using VBI systems; offenders will be subject to the penalties defined by the Commission, in accordance with Item 14 below;

(ii) Any identity is individual, personal, and non-transferrable and each Associate is responsible for properly storing and ensuring absolute confidentiality of such identification. The use of identification is limited to the purposes described in the statement of responsibility for each access control;

(iii) VBI reserves the right to monitor the traffic of data and any information flowing through its communication network;

(iv) In order to be considered secure, equipment, systems, and peripherals must have been approved by the IT Manager and the Commission prior to their installation and/or use; market ratings are insufficient for internal use;

(v) Equipment used to carry out VBI activities must always be up to date, including operating systems, antivirus, and firewalls, in order to protect information contained in such equipment;

(vi) Backups must be made of VBI's electronic data repositories, with regular updates, based on the highest security standards available in the market;

(vii) All Associates must notify the commission if they witness, know, or even suspect of any fact that violates the rules specified in this Policy, in the existing legislation, and in any instructions given by this Commission, as per Item 15 below;

(viii) The granting of access to Confidential Information must follow the criteria of least privilege, under which users have access only to information resources essential to the full performance of their activities;

(ix) Any Associate receiving Confidential Information must keep such information in confidence, limiting their access and controlling any copies;

(x) Access to Confidential Information must be controlled using the signature of confidentiality agreements, as per Item 13 below; and

(xi) No change in the technical settings of the software that may jeopardize the degree of security or prevent or impair the monitoring of such software by the IT Manager or the Commission is permitted.

4.3 ALLOWED DISCLOSURES

The following disclosures of Confidential Information will not be considered violations of this Policy: (i) because of legal or regulatory requirements; (ii) by the Associate, provided to the extent strictly necessary to perform their duties, including but not limited to disclosure to lawyers and independent auditors and counterparties; and (iii) to comply with orders by any regulatory, administrative, legislative, judiciary, or arbitral authorities of competent jurisdiction, at the local, state, district, or federal levels; in the case of Item "(iii)" this disclosure to such individuals must be reviewed in advance by the Commission.

4.4 POLICY REGULATION

Periodically, the Commission may issue rules to regulate the provisions of this Policy in order to ensure its performance; examples include but are not limited to defining internet pages whose access is blocked, and systems, equipment, and peripherals approved by the Commission for professional use.

5. INTERNET USE RULES

For VBI, the internet is considered a high-risk connection; accordingly, it is of the utmost importance that when browsing the internet users are aware that they may be placing at risk the confidentiality, integrity, and availability of VBI assets.

The IT Manager is responsible for monitoring access to websites using VBI-owned computers and devices to assess any possible improper use and block access to banned websites.

Associates must use the internet in a professional and honest manner and following the requirements below:

(i) All network and internet access control means must be respected;

(ii) Under no event may any information or data of interest to VBI be disclosed, facilitated, or shared, whether confidential or otherwise, in forums, discussion lists, chat rooms, or any other means using the internet, except when authorized by the VBI Board;

(iii) Under no event may any system, software, or data be uploaded without authorization of the IT Manager or the Commission, except when such disclosure is authorized in accordance with Item 4.3 above, for legal and/or regulatory purposes;

(iv) The download of systems and data from the internet must always rely on good sense and comply with licensing agreements, terms of use, and privacy policies applicable thereto; Associates must always check with the IT Manager prior to downloading any data or system when there is any doubt regarding the legitimacy of the source or suspected contamination of malicious programs;

(v) At the request of the VBI Board, the IT Manager can implement the production of reports on the internet webpages visited and the identification of those visiting those pages;

(vi) The Associate is personally responsible for all activities carried out using their login, password, and other access data;

(vii) Internet access outside the workplace using VBI equipment or peripherals must be made for professional purposes only because of meetings or remote working or any other situations previously approved by the VBI Board and provided the parameters defined by the Commission are complied with;

(viii) Absolutely no websites or systems are to be accessed with VBI equipment and peripherals using proxies.

6. EMAIL USE RULES

Each user will be responsible for the corporate email account provided by VBI; such account must be used diligently, ethically, and professionally.

Associates must follow the good practices listed below when using their email:

(i) Send email messages only to personnel involved in the matter discussed, making sure only the right addresses are entered;

(ii) Print email messages only when necessary;

(iii) When Associates receive any messages that violate the rules defined by VBI, with suspicious titles or exhibits, such messages should never be forwarded and the individual in charge of their area or the IT Manager should be advised, as necessary;

(iv) When leaving their workstations, even if temporarily, Associates must block their workstation; and

(v) When leaving on vacation or extended planned leaves, Employees must use the temporary out of office autoresponder functionality in their email.

Under no event should Associates:

(i) Use email to send files or transmit confidential information, except in the cases described in Item 4.3 above;

(ii) Send spam, chain emails, or similar messages;

(iii) Send any material with anonymous content;

(iv) Send emails with content that violates VBI's Code of Conduct and Ethics, contains any threat, libel, slander, injury, extorsion, requests or acceptance of bribes, or any other type of offense specified under existing law;

(v) Send malicious code of any type whatsoever, such as trojan horses, virus, etc.;

(vi) Send to any third parties, for any reason whatsoever, the list of VBI email addresses;

(vii) Send or open any executable files received with extensions such as .exe, .dat, .dll, .com, .bat, .pif, .is, .hta, and .src;

(viii) Use private email accounts with POP, IMAP, and SMTP servers;

(ix) Forward advertisements or advertise any private products or services using the corporate email; and

(x) Forward their personal email or any mail from other providers to their corporate email inbox or vice-versa.

VBI will have unrestricted access to all emails sent and received by its Associates using the corporate email account.

7. CONTROL OF LOGINS AND PASSWORDS

All passwords are personal and should not be disclosed at the penalty of the Associate being warned or dismissed for cause, in addition to any applicable administrative and criminal penalties. The same rules apply to passwords used by more than one Associate.

The password must be memorized and cannot be available on physical means or on the network, at the penalty of the Associate being warned or dismissed for cause if the password becomes known to any third party because of fault or malice of the user.

The access login and password will consist of at least eight characters; it is suggested that they include alphanumeric characters and special characters.

Any accounts that remain inactive for over 90 days will be automatically blocked or forwarded to other email inboxes, as the convenience of VBI.

VBI may determine a minimum mandatory frequency to change the passwords.

When an Associate leaves the company, their accesses (including logins and passwords) to internal systems will be blocked.

Managers of each area must communicate the IT Department of any changes in activities of Associates under their responsibility and the need for reviewing their accesses as a result of such changes.

8. CONTROL OF PHYSICAL ACCESS TO INFORMATION AND DATA

Absolutely no confidential or restricted material should be left on desks or workplaces after business hours; no information should be left on whiteboards in meeting rooms after the meeting is closed. When using shared printers, the printed document must be immediately retrieved.

Each Associate is responsible for any material sent outside the company for printing; such Associate will be responsible for any Confidential Information lost or leaked, and any such occurrences must be immediately reported to the Commission.

All material containing Confidential Information and data must be destroyed after its use, as applicable.

File cabinets used to store physical documents must remain locked and the key entrusted to an responsible individual.

Associates must destroy all material containing Confidential Information and data, using the following techniques:

(i) Written or printed documents must be shredded in suitable machines; in the absence of paper shredders, the documents must be destroyed until they become illegible and unrestorable;

(ii) CDs, computer chips, and electromagnetic media must be destroyed physically, preferably be shredded or if this is not possible broken into at least six parts; and

(iii) Hard disks or peripheral components should be destroyed using a punching or cutting tools, preferably a hammer drill.

9. CLOUD COMPUTING

Cloud data storage or computing services hired by VBI must undergo a strict internal selection process, which will review the need for outsourcing this service and the technical reliability of the service in question to ensure they have the required security qualifications.

Associates should not use cloud computing systems without the prior and express consent of the IT Manager and the Commission.

10. CONTROL TESTS

The effectiveness of this Policy is checked using regular tests of the existing controls, at least once a year, under the responsibility of the Information Technology Department, which will report the findings to the Commission. The tests should check whether:

(i) Human and computer resources are suitable to the size and areas of operation;

(ii) There is a proper level of confidentiality and accesses to Confidential Information, with the identification of individuals who have access to such information;

(iii) There is physical and logical segregation;

(iv) Computer, control, and physical and logical access resources are protected; and

(v) Records maintenance allows for audits and inspections.

11. TERM AND COMMUNICATION

This Policy will become effective on the date it is published and will remain in effect for an undetermined term.

This Policy revokes and replaces all prior versions and any other prior provisions in any other documents contrary to the provisions in this Policy regarding this subject matter.

This Policy and any other supplementary regulations issued by the Commission, as per Item 4.4 above, will be reviewed and updated as necessary at least once a year by the Commission and anytime it is appropriate or necessary as a result of superseding law or regulations.

11.1 COMMUNICATION

This Policy as well as any changes will be made available on the VBI page on the internet and communicated to all Associates of VBI as of the date it becomes effective.

VBI will present this Policy to ANDIMA in the ways this authority determines as of the date the Plan becomes effective and, if there are any changes, within fifteen (15) calendar days after such change, pursuant to Article 86 of the ANDIMA Code, or lesser time to determined by ANDIMA.

VBI will provide copies of this Policy to all other supervisory authorities (including but not limited to CVM and ABVCAP, as applicable) whenever asked, in accordance with applicable law and regulations.

12. COMMUNICATION AND TRAINING

12.1 COMMUNICATION TO THE REGULATORY AND SELF-REGULATORY AUTHORITIES

Any nonconformity regarding issues of personal and professional conduct must be submitted to the VBI Compliance Committee for review and decision on the steps to be taken.
The Director of Internal Controls must inform applicable oversight, regulatory, and self-regulatory authorities (including but not limited to CVM, ANBIMA, and ABVCAP, as applicable) anytime he/she, in the exercise of their duties, identifies an occurrence or signs of violation of any law these authorities

enforce, within ten (10) working days of the occurrence or identification, or lesser time defined under other VBI policies or law or regulations in effect at the time of such facts.

12.2 PROFESSIONAL TRAINING AND EDUCATION

When joining the company, all VBI Associates will be trained on this Policy.

All Associates will undergo mandatory training at least once a year or as necessary as a result of changes in law or of material fact; this training will be coordinated by the IT Manager and will communicate updates on this Policy and reinforce in the team the understanding and the need to observe the rules specified above.

Each training will be recorded and will include an attendance sheet, which will be filed in a digital folder related to this matter; the Associate attendance will be recorded in a list attached to the minutes of such meeting.

13. CONFIDENTIALITY AGREEMENT

Each VBI Associate will receive a Confidentiality Agreement under which such Associate will promise to maintain the secrecy of all Confidential Information; this Confidentiality Agreement must be signed by the Associate and submitted to the Committee, which will file this document; the sample of this Confidentiality Agreement is shown in Exhibit A of this Policy.

Suppliers, service providers, and other third parties must also enter such Confidentiality Agreement and submit it to the Commission before such personnel has access to any Confidential Information.

14. PENALTIES

Failing to comply with this Policy represents serious misconduct and may result in the following penalties: formal warning, suspension, termination of the employment contract, other disciplinary action, and/or civil or criminal prosecution.

To the extent allowed under the law, VBI will not be responsible before any third parties for Associates who have violated the law or committed violations in the performance of their duties. In case VBI is penalized or has a loss of any nature as a result of the actions of its Associates or third parties, VBI may exercise its rights of redress or indemnity against the parties responsible.

15. QUESTIONS, GUIDANCE, AND COMMUNICATION OF INCIDENTS

Regarding this Policy, any request involving clarification or guidance by the Commission must be emailed to controlesinternos@vbirealestate.com or through the Compliance Channel of the Compliasset System.

In case any information is leaked or improperly accessed, the Commission must be immediately informed to take the necessary steps, which will range from a reprimand for such access or message

sent to the wrong recipient to instruct such Associate to exclude the respective content (if applicable), to a review and actual implementation of legal steps, as applicable, notwithstanding any investigation of the facts and possible penalties to the Associates involved.

16. REVISION HISTORY

Below is a table indicating the history of revisions to this Policy:

Version	Approval Date
1	September 2011.
2	August 2016
3	July 13th , 2021.

EXHIBIT A
CONFIDENTIALITY TERM

Name:		
Area:	Position:	
Identity - Nº:	Type:	CPF:

I hereby declare that I read the Information Security Policy ("Polícy") of VBI Real Estate Gestão de Carteiras Ltda. ("VBI"), applicable to VBI and/or, when the context allows, its controlling companies, and I am aware of its content, which is directly linked to the performance of my roles.

Pursuant to this term I hereby commit to:

(i) maintain confidentiality of the information that is not public, produced or kept by VBI or that I have access due to my role in VBI ("Confidential Information");

(ii) not to disclose to any person, unless expressly authorized by VBI or in case necessary to the performance of my role in benefit of VBI, any Confidential Information;

(iii) immediately destroy, as per VBI´s request, any material or document containing Confidential Information;

(iv) not to use any Confidential Information in its own benefit or for the benefit of third parties;

(v) immediately inform VBI any violation of the present Term or any disclosure due to demand of authorities or judicial or administrative order.

_____, _____ de _____ de 20_____.

_____
Associate Signature

EXHIBIT IV – CONTINGENCY AND BUSINESS CONTINUITY PLAN

1. DEFINITIONS

The terms used in this document starting in capital letters have the meanings shown below. If not shown here, they will have the meanings attributed to them under VBI's Rules, Procedures, and Internal Controls Manual.

"Commission"	Means the Internal Controls and Risk Management Commission.
"Plan"	Means this Contingency and Business Continuity Plan.
"Systems"	Means any and all operational systems used by VBI Associates in the performance of their duties.

2. OBJECTIVE

This document was prepared to ensure the continuity of VBI's operational work and businesses in situations in which VBI's operational systems are inoperative or, for some reason, the Associates are prevented from or unable to enter VBI's physical facilities, helping those involved in the contingency plan to take action and carry out the necessary procedures until the normal working conditions and VBI systems are restored.

Associate awareness of and familiarity with this plan and the critical points it mentions will help diagnose the problems and find their solutions.

3. SCOPE

The contents of this document must be known to and obeyed by all VBI Associates. Each Associate must comply with its guidelines and rules and make sure they are complied with by third parties (including visitors and service providers) who, under their responsibility, have access to VBI's facilities or systems.

4. RESPONSIBILITIES

The Commission will monitor compliance with this Plan and supervise the regular tests specified in Item 0 below.

In case of any discrepancies, the Board of VBI will meet in person or remotely to trigger the contingency plan.

5. PREVENTIVE CONTROLS

VBI maintains internal and external facilities to minimize the risks of its activities being interrupted, including but not limited to those listed below.

5.1. INTERNAL PREVENTIVE CONTROLS

(i) Daily online backup of all information and user setups in a local data center;

(ii) Access control system to VBI's premises;

(iii) A datacenter fitted with access control, dedicated air-conditioning, redundant telecommunication links with different providers, firewall, antivirus, and backup system in a remote location;

(iv) Uninterrupted power supply systems for the datacenter and workstations.

5.2. EXTERNAL PREVENTIVE CONTROLS

(i) Information and electronic versions of documents relative to investment funds managed by VBI are fully or partially replicated in the external repositories of the respective administrators and custodians of such funds;

(ii) External datacenter provided by a contractor.

6. PROCEDURES

The Plan includes regular and specific procedures to prevent and address contingencies, as shown below.

6.1. REGULAR PROCEDURES

(i) Once a year or as necessary, in response to new activities or systems, the Commission will oversee the identification and reassessment of the positions, critical systems, and potential risks; and

(ii) Once a year or at shorter intervals, the Commission will oversee tests of this Plan, as shown in Item 0 below.

6.2. PROCEDURES TO ADDRESS CONTINGENCIES

In this order:

(i) When any incident is identified, the Associate must notify the Internal Controls and Compliance Director, who in turn will notify the Board and/or the Commission, depending on the severity of the incident;

(ii) The Board will decide whether to invoke the Plan; in case yes, it will decide on what steps will be taken to maintain operations;

(iii) The Board will communicate Associates what steps will be taken while the incident lasts; in time, it will communicate the business resumption plan;

(iv) After the incident ends, the IT Manager must report to the Board what caused the incident should the origin not be known immediately; the steps taken and their degree of success must also be reported;

(v) After reviewing the information reported, the Commission will decide on the need to hold new tests and adjust the Plan.

7. PREVENTIVE ANALYSIS

The Commission will oversee regular tests of the Plan with (i) the IT team, including the probability of interruption or malfunctioning of local and external systems, power supply equipment (including uninterrupted power supply systems), and telephone systems; (ii) building management regarding the risks to VBI's physical installations.

In case any tests identify a possible malfunction, the IT Manager must immediately notify the Commission for preventive adjustments.

8. CORRECTIVE STEPS

As an example, the Commission can take the steps described below to respond to incidents. Other steps can be identified and listed in a document issued by the Board and/or the Commission.

8.1. TOTAL SYSTEM FAILURE

In this case, all Systems are impacted. The Commission will check the "general failure" diagnostic, shut down and restart everything, and confirm whether the situation persists. If the situation persists, the Commission must meet as soon as possible to discuss the best way of restoring the Systems.

8.2. PARTIAL SYSTEM FAILURE

In this case, some Systems are impacted. The Commission must identify which Systems are being impacted, diagnose the causes, and identify possible solutions and competences for technical interventions.

8.3.POWER SHORTAGES

Within four (4) hours after a power shortage starts, the Commission must identify the extent and the possible causes located. The Commission will:

(i) In case it is a local problem, enable an immediate solution; and

(ii) If the problem is not local and an immediate solution is not feasible, the Associates must be instructed to work remotely from their homes.

8.4. TELEPHONE SYSTEM FAILURE

As required, the Commission will request service to the telephone provider; Associates will be instructed to adopt the following workaround steps to service over the telephone:

(i) In case of intermittent service caused by power shortages:

(a) Associates may continue providing service while the uninterrupted power supply last, which is about four hours; and

(b) In case the power shortage extends for a longer period, Associates will use the cellphone network and reroute calls from the landlines to the mobile lines or to other Associates not

impacted by the shortage.

(ii) In case of interrupted landline service:

(a) Associates will use the cellphone network to provide service and reroute calls from the landlines to the mobile lines or to other Associates not impacted by the interrupted landline service.

8.5. LACK OF DATA OR INFORMATION FROM INFORMATION PROVIDERS

The Board or the Commission must contact the providers as soon as possible to identify the causes and possible contributions to restore the signal.

Use information obtained over the internet.

8.6. FINANCIAL CLEARING – BANKS AND SUPPLIERS

(i) When access to the office is prevented:

(a) Associates will access banks using online banking, if available; and

(b) Associates authorized to access the VBI server remotely will work from their homes.

(ii) In case of power shortages:

(a) Associates may continue providing service while the uninterrupted power supply last, which is about four hours; and

(b) Associates authorized to access the VBI server remotely will work from their homes.

9. TERM AND COMMUNICATION

This Plan will become effective on the date it is published and will remain in effect for an undetermined term.

This Plan revokes and replaces all prior versions and any other prior provisions in any other documents contrary to the provisions in this Plan regarding this subject matter.

This Plan and any other supplementary documents issued by the Commission, as per Item 0 above, will be reviewed and updated as necessary at least once a year by the Commission and anytime it is necessary as a result of superseding law or regulations.

9.1. COMMUNICATION

This Plan as well as any changes will be made available on the VBI page on the internet and communicated to all Associates of VBI as of the date it becomes effective and at the Compliasset System.

VBI will present this Plan to ANDIMA in the ways this authority determines as of the date the Plan becomes effective and, if there are any changes, within fifteen (15) calendar days after such change, pursuant to Article 86 of the ANDIMA Code, or lesser time to determined by ANDIMA.

VBI will provide copies of this Plan to all other supervisory authorities (including but not limited to CVM and ABVCAP, as applicable) whenever asked, in accordance with applicable law and regulations.

10. QUESTIONS, GUIDANCE, AND COMMUNICATION OF INCIDENTS

Regarding this Plan, any request involving clarification or guidance by the Commission must be emailed to ti@vbirealestate.com.

11. REVISION HISTORY

Below is a table indicating the history of revisions to this Policy:

Version	Approval Date
1	September 2011.
2	August 2016
3	July 13th , 2021.

EXHIBIT V – SEGREGATION OF DUTIES POLICY

1. DEFINITIONS

The terms used in this document starting in capital letters have the meanings shown below. If not shown here, they will have the meanings attributed to them under VBI's Rules, Procedures, and Internal Controls Manual.

"Commission"	Means the Internal Controls and Risk Management Commission.
"Policy"	Means this Segregation of Duties Policy

2. OBJECTIVE

This Policy formalizes rules and procedures to be followed in the physical and functional segregation of duties in the management of securities portfolios from other duties performed by VBI, as applicable and pursuant to existing law.

The objectives that guide this Policy are:

(i) Mitigate the occurrence of acts that are illegal or violate regulations;

(ii) Segregate functions in the areas responsible for managing portfolios from other areas that could bring conflicts of interest, in order to properly minimize such conflicts;

(iii) Ensure physical segregation of facilities between the area responsible for managing portfolio and – when these duties are performed by VBI – the area responsible for intermediation and distribution of financial assets;

(iv) Encourage the proper use of installations, equipment, and information shared by more than one area of the company;

(v) Preserve confidential information and allow identification of the individuals with access to such information; and

(vi) Properly manage and monitor the areas identified as having possible conflicts of interest.

3. SCOPE

The contents of this document must be known to and obeyed by all VBI Associates. Each Associate must comply with its guidelines and rules and make sure they are complied with by third parties (including visitors and service providers) who, under their responsibility, have access to VBI's facilities or systems.

VBI's Information Security Policy supplements the rules and procedures relative to the segregation of duties of the organization; this document should also be known to and obeyed by all VBI Associates.

4. SEGREGATION OF DUTIES

VBI's activities are segregated in the manner described below. Any exceptions must be previously

requested to the [Commission], which may or may not agree with the requests, based on the relevance and need of the action.

4.1. PHYSICAL SEGREGATION

The physical space used by portfolio management is restricted to those in charge of this work; the corresponding files and confidential information must be absolutely separated, and access must be restricted through the use of individual identification badges.

4.2. VIRTUAL ACCESS

Each Associate's access is restricted based on the team of which such individual is part and on their hierarchical level. This means that only Associates duly authorized will have access to the systems as well as to the files, directories, and/or folders in the VBI network, using physical and logical segregation.

Segregation and protection measures further include standards for defining passwords with proper complexity, audit trails in the network and in the systems used, so that any individuals accessing such data can be identified; regular backups must preserve information and ensure its security.

4.3. RESTRICTION TO THE CIRCULATION OF CONFIDENTIAL INFORMATION

Information to which Associates may have access as a result of their duties cannot be transferred to unauthorized people or any individuals who may use such information improperly, whether they be other Associates or otherwise, always in accordance with the other rules and permissions to disclose confidential information as provided in VBI's Information Security Policy.

5. CONTROL TESTS

The effectiveness of this Policy is checked using regular tests of the existing controls, at least once a year, under the responsibility of the Compliance Committee with the help of the IT Manager. The tests should check whether:

(vi) Human and computer resources are suitable to the size and areas of operation;

(vii) There is a proper level of confidentiality and accesses to Confidential Information, with the identification of individuals who have access to such information;

(viii) There is physical, logical, and functional segregation;

(ix) Computer, control, and physical and logical access resources are protected; and

(x) Records maintenance allows for audits and inspections.

6. TERM AND COMMUNICATION

This Policy will become effective on the date it is published and will remain in effect for an undetermined term.

This Policy revokes and replaces all prior versions and any other prior provisions in any other documents contrary to the provisions in this Policy regarding this subject matter.

This Policy will be reviewed and updated as necessary at least once a year by the Compliance Commission and anytime it is appropriate or required under superseding law or regulations.

6.1. COMMUNICATION

This Policy as well as any changes will be made available on the VBI page on the internet and communicated to all Associates of VBI as of the date it becomes effective.

VBI will present this Policy to ANDIMA in the ways this authority determines as of the date the Plan becomes effective and, if there are any changes, within fifteen (15) calendar days after such change, pursuant to Article 86 of the ANDIMA Code, or lesser time to determined by ANDIMA.

VBI will provide copies of this Policy to all other supervisory authorities (including but not limited to CVM and ABVCAP, as applicable) whenever asked, in accordance with applicable law and regulations.

7. PENALTIES

Failing to comply with this Policy represents serious misconduct and may result in the following penalties: formal warning, suspension, termination of the employment contract, other disciplinary action, and/or civil or criminal prosecution.

To the extent allowed under the law, VBI will not be responsible before any third parties for Associates who have violated the law or committed violations in the performance of their duties. In case VBI is penalized or has a loss of any nature as a result of the actions of its Associates or third parties, VBI may exercise its rights of redress or indemnity against the parties responsible.

8. QUESTIONS, GUIDANCE, AND COMMUNICATION OF INCIDENTS

Regarding this Policy, any request involving clarification or guidance by the Commission must be emailed to compliance@vbirealestate.com or through the Compliance Channel of the Compliasset System.

EXHIBIT IV - EXTERNAL ACTIVITIES POLICY

1. DEFINITIONS

The terms used in this document, starting with capital letters, have the meanings indicated in the table below, or, if not defined herein, those assigned in the VBI Rules, Procedures and Internal Controls Manual.

"External Activities"	"It means activities carried out by Employees, for profit or not, in any organization, group or company in which VBI is not a shareholder or quotaholder and the activity is not related to the function performed by the Associate in the Manager, outside the Manager's premises. This includes, but is not limited to, the following activities: (i) Outside employment; (ii) Participation in boards or committees of companies or organizations; (iii) Ownership or active participation in a private business; (iv) Significant civic or charitable involvement or activity; (v) Any other activity that may affect the impartiality of the VBI Associate."
"Policy"	It means this External Activities Policy.

2. OBJECTIVE

To mitigate the risks linked to the exercise of certain External Activities, such as the risk of conflicts of interest, risk of inducing customers to error or even reputational, legal or regulatory risk, VBI divides external activities into 3 (three) categories: (i) external activities exempt from communication or approval; (ii) external activities that need approval; and (iii) prohibited outside activities.

3. EXTERNAL ACTIVITIES EXEMPT FROM COMMUNICATION OR APPROVAL

The External Activities described below do not need to be communicated or approved by the Internal Controls Department:

- Outside teaching jobs;
- Participation in sports teams, except nationally renowned football clubs;
- Recreational artistic activity;
- Musical group; and
- Activities involving the Third Sector.

4. EXTERNAL ACTIVITIES THAT REQUIRE COMMUNICATION AND APPROVAL

- Holding management positions or other positions in any companies, including publicly traded companies;
- Participation in the Board of Directors or Fiscal Council, Committee or any of the management bodies, or with technical and advisory functions in a publicly held company;

• Employment ties with other institutions, companies or people;
• Consulting activities or provision of services of any nature, such as legal consulting, lectures and writing articles for public media (in this case, pay attention to the internal policies of contact with the media and publication of material); and
• Any activities not described in one of the fields of this Policy.

5. PROHIBITED OUTSIDE ACTIVITIES

• Position, employment or role with a competitor or other market participant;
• Occupation in political or public office, employment or function;
• Activities that may expose the image of the VBI (e.g. participation in reality shows, radio and TV programs); and
• Activities aimed at adults and nudity.

6. COMMUNICATION AND APPROVAL PROCESS

For activities that require communication and approval, communication with the Internal Controls Department must be done via the email compliance@vbirealestate.com or through the Compliance Channel of the Compliasset System and must bring the following information:

• Name of the Associate;
• Area of Operation within the VBI;
• Immediate superior; and
• Description of the external activity.

Associates must also request approval from the Internal Controls Department for any new external activity to be developed that depends on approval, even if in the same company or institution previously approved. In addition, the Internal Controls and Compliance Officer must be informed if there is any change in External Activities already approved by the Internal Controls Department.

The Internal Controls Department will analyze the case and, from now on, make it clear that it may deny the approval of external activities whenever it understands, at its sole discretion, that such activities represent risks or conflicts of interest to the Manager. Likewise, the Manager may request the immediate termination of external activities.

7. TERM AND DISCLOSURE

This Policy will enter into force on the date of its publication and will remain in effect for an indefinite period.

This Policy revokes and replaces all its previous versions as well as any other previous provisions contrary to the provisions of this Policy contained in any other documents, regarding its object.

This Policy will be reviewed, as necessary, at least annually by the Commission and, also, whenever opportune or mandatory due to supervening legislation or regulation. The recommendations for updating this Policy will be submitted for approval by the VBI Board of Directors, pursuant to the VBI Rules, Procedures and Internal Controls Manual.

7.1. DISCLOSURE

This Policy, as well as any amendments thereto, are available on the VBI network (at "VBIREALESTATE/COMPLIANCE/POLICIES") and will be made available on the VBI website and disclosed to all VBI Collaborators as of its entry into force through of the Compliasset System.

VBI will make a copy of this Policy available to other inspection entities (including, without limitation, CVM and ABVCAP, as applicable) whenever requested, under the terms of applicable legislation and regulations.

8. PENALTIES

Failure to comply with this Policy implies serious misconduct and may result in the following penalties: formal warning, suspension, termination of employment, other disciplinary action and/or civil or criminal proceedings.

To the maximum extent permitted by law, VBI will not be liable to third parties for Associates who violate the law or commit infractions in the performance of their activities. If VBI is penalized or suffers damages of any nature due to the actions of its Associates or third parties, it may exercise the right of recourse or compensation against those responsible.

9. DOUBTS, GUIDELINES AND REPORTING OF OCCURRENCES

In relation to this Policy, any request that involves guidance or clarification by the Commission must be sent to the email: compliance@vbirealestate.com or through the Compliance Channel of the Compliasset System.

All Employees are responsible for informing the Compliance Committee, through the email address above or through the Whistleblower Channel, of any suspected cases of activities that violate this Plan.

10. REVISION HISTORY

Below is a table indicating the history of revisions to this Policy:

Version	Approval Date
1.	July, 13th, 2021.