

**INFORMATION SECURITY AND TREATMENT OF PERSONAL DATA POLICY****IG4 CAPITAL INVESTIMENTOS LTDA.**

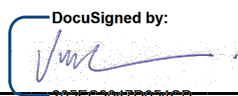
("Manager")

Current version: June/2022

Previous version: July/2021

Document No.:	Review No.:	Effectiveness:
1	6 (June 2022)	11/30/2016, and, when applicable, as from obtainment of CVM consent to operate as fund manager

Approved by: _____

DocuSigned by:

203EC0047D054CD...

Flávia Andraus Troyano**Compliance Officer****CHAPTER I
PURPOSE**

1.1. This instrument is intended to formalize the Information Security Policy ("Policy") adopted by the Manager, in a permanent manner, in order to present and disseminate among the Workers the control procedures used to guarantee the security of information produced and managed in the work environment of IG4 Capital.

1.2. Therefore, it is a responsibility of every Worker guaranteeing the confidentiality and completeness of the information produced during the development of work at the Manager, being essential that all Workers are fully aware of the importance of each one to guarantee the effectiveness of the procedures defined in this Policy.

1.3. Commitment to comply with this Policy is also demanded from all Workers of IG4 Capital.

1.4. Any Worker who becomes aware of any violation of this Policy must report it to the Department of Compliance through the e-mail compliance@ig4capital.com or report it through the Reporting Channel of the Manager.

CHAPTER II

SCOPE

2.1. "Workers", in line with the concept defined by the Code of Ethics and Conduct of the Manager, are understood as: (i) partners and associates; (ii) employees; (iii) officers; (iv) interns; or (v) any people who, due to their jobs, functions or positions at the Manager, have access to information generated internally and or received from clients for the development of internal work.

2.2. Every Worker must be aware that all information generated internally or received is strictly confidential. Accountability for confidentiality and completeness of such information shall remain in force even after termination of the working relationship with the Worker, and failing to comply with the provisions provided for in this Policy shall be considered as a severe infraction, subject to administrative and/or legal sanctions.

CHAPTER III

GUIDELINES AND PROCEDURES

3.1. Access Control:

Information exchange among Workers of the Manager must always be based on the concept that the recipient must be someone who needs to receive such information for the development of their activities and is not subject to any barrier that impedes them from receiving such information. In case of doubts, the Department of Compliance must be contacted previously to the revelation.

In order to guarantee control over Confidential Information, the following measures are used:

- (i) login and password to access the network of individual computers for each Worker, as well as to access e-mail and mobile devices used for working, and such passwords are personal and non-transferable;
- (ii) prohibition of connecting equipment not previously authorized by the computing area of the Manager into the network of the Manager, and the Workers are not allowed to use computers, external hard drives or any other

devices not related to the development of their activities at the Manager;

- (iii) electronic information network with the use of exclusive servers of the Manager, preventing access by third parties;
- (iv) maintenance of different levels of access to electronic folders and files according to the jobs of the Workers, with log of access to such folders and files by the Workers based on the password and login of each Worker, and protection against tampering and maintenance of records that enable audits and inspections;
- (v) monitoring access to websites, blogs, fotologs and webmails, and more, as well as e-mails sent and received;
- (vi) monitoring, also by means such as recordings of telephone calls made or received in the telephone lines made available by the Manager for the professional activity of each Worker; and
- (vii) access blocking to the systems by the IT department, upon request of the Department of Compliance, or in case any risk for the network or systems of the Manager is detected by the IT department.

Workers may be held accountable in case they provide any of their passwords to third parties.

The information technology department ("IT") shall make biannual checks in the corporate network of the Manager, in order to validate safe access to the resources available, good use of equipment and information shared by more than one sector of the Manager, safeguard of Confidential Information and identification of the people who had or have access to them, protection against tampering and maintenance of records that enable audits and inspections. At the end of each check, an e-mail shall be forwarded by the IT Area to the Department of Compliance, reporting the conclusion of the tests performed, including occasional irregularities or failures identified.

Regarding physical copies, documents containing Confidential Information must be in an archive with restricted access and must be ground before being disposed of, preventing undue access to such information, observing the rules related to conservation of documents for applicable legal periods.

The headquarters of the Manager has physical segregation of spaces, so that (i) access to the space allocated to the management activity is restrict to the respective Workers; (ii) meetings, including those with non-workers, are held in a reserved manner, in specific rooms segregated from the space allocated to the management

activity.

3.2. Backup:

All documents filed in the computers of the Manager are subject to daily backup in the cloud with control of the changes made in the files, guaranteeing the safety of the respective content and eventual accountability.

3.3. Copy of files and installations:

All computer programs used by the Workers must be previously authorized by the person in charge for the IT Area. Downloads of any nature are allowed, upon justification.

File copying and installation of programs in computers of the Manager must respect relevant intellectual property rights, such as licenses and patents.

The Workers are strictly forbidden from making copies (physical or electronic) or printing the files used, generated or available in the network and circulate in external environments with such files, except for the purposes of the execution and development of business and interests of the Manager. In such cases, the Worker who is in the possession and guard of the file is directly responsible for its safeguard, integrity and maintenance of its confidentiality.

Any document printing must be immediately removed from the printer, as it may contain restricted and confidential information even in the internal environment of the Manager. Keeping such printings on desks, fax machines or copy machines is also prohibited.

3.4. Disposing of Information:

Disposing of confidential information must follow the guidelines below:

- (i) the disposed content must be deleted and/or the media must be destroyed, to its recovery impossible, so that the information is not vulnerable to unauthorized access;
- (ii) physical documents containing protected information must be ground immediately after being used, in order to prevent their recovery or reading;
- (iii) elimination or final destruction of media or documents, carried out by third parties, must be documented.

- (iv) memory devices and storage devices (for example, laptops, USB devices, portable hard drives, tablets, smartphones) deactivated by the Manager must be erased so that the protected information contained in them is irrecoverable.

3.5. Redundancy:

In addition to the aforementioned security copies, other IT resources are redundant. In the event of failure or unavailability of physical access to the workplace, the team may access the information in the cloud from any location.

In order to guarantee proper work of the network and data integrity, even in an occasional interruption of electric energy supply, all work stations and the server are connected to an equipment like a no-break, which enables the network to keep working long enough so that the users save their files.

3.6. Support and Monitoring:

In the event of failure in the network or any work station, the fact must be immediately reported to the IT Area, which shall ensure internal support or make arrangements to trigger the required external support.

The electronic systems used by the Manager are subject to review and monitoring at any time, without warning or permission, in order to detect any irregularities in information transfers, either internally or externally;

In that sense, considering that the use of e-mail is intended exclusively for professional purposes, as a tool to develop the Workers' activities, the Manager may also monitor each and every exchange, either internal or external, of e-mails by the Workers.

Any suspected or known violation of this Policy or information security incident must be reported to the Compliance Area in order to take suitable measures related to the investigation of the facts, mitigation of risks, implementation of corrective procedures and accountability of the individuals involved.

The Manager may carry out, periodically and with no warning, inspections in the computers to check downloads that may be improper, unauthorized or stored in inadequate locations.

3.7. Treatment of cases of confidential information leakage:

In the event of leakage of confidential information related to investors, or any other Personal Data or Sensitive Personal Data treated by the Manager (Data Treatment rule, coming next), even when arising from an involuntary action, the Compliance Officer

shall notify the interested parties about the occurrence. When it comes to Personal Data or Sensitive Personal Data, the Data Protection National Authority must be communicated as well, in addition to the owner of the data. Such communication shall meet the parameters demanded by the Data Protection General Law.

Notwithstanding, the Manager shall activate its Recovery Plan aiming at identifying the cause that led to the leakage and to hold the perpetrator accountable. Moreover, a report about the damage incurred, percentage of activities affected, financial impact, suggesting, in addition, measures to be taken in order to enable the activities to be normally resumed, shall be prepared.

Such reports shall be prepared by the Compliance Officer and shall be submitted to the Executive Board of the Manager in order to promote suitable initiatives to return to normality as soon as possible.

3.8. Firewall:

The Manager uses Firewall technology to protect its network against outside threats.

3.9. Security Tests:

The following security tests are carried out to monitor the systems used:

Test	Periodicity
Control of connected devices	On demand
Access Control	Annual
Double authentication tests	Monthly

CHAPTER IV
TREATMENT OF PERSONAL AND SENSITIVE DATA

4.1. The Manager is watchful for observing, implementing and complying with rules, policies and procedures related to Information Security.

4.2. Notwithstanding the guidelines contained in the aforementioned Information Security Policy and with the purpose of protecting the fundamental rights of freedom and privacy, the Manager adopts rules and procedures for the treatment of personal data and, occasionally, sensitive data, including those in digital media, in line with the General Data Protection Law. The following definitions are considered for the purposes of this Code:

- “Personal Data” is any information related to an identified or identifiable individual.

- “Sensitive Personal Data” is Personal Data related to racial or ethnic background, religious belief, political opinion, affiliation a union or an organization of religious, philosophic or political nature, data related to health or sexual habits, genetic or biometric data, when connected to an individual.

4.3. Every Personal Data or Sensitive Personal Data is Confidential Information and must be treated as such for the purposes of this Code and other manuals and internal policies adopted by the Manager.

4.4. Treatment of personal data and sensitive data shall be carried out exclusively: (i) for the purposes of complying with regulatory obligation, due to normative demands issued by CVM and self-regulatory issued by ANBIMA; or (ii) to carry out a contract signed with a client. In any case, client information shall be collected solely for legitimate purposes, aiming at providing services hired by the client or complying with regulation and self-regulation, and the Manager shall keep record of the operations of treatment of personal data and sensitive personal data it performs.

4.5. When treatment of Personal Data or Sensitive Personal Data is required for purposes different from those defined above, consent shall be collected from the owner of the data, in writing or by any other way that expresses manifested will, for the treatment of their data, and the purposes it is intended to must be expressly identified. In that case, the owner of the data (personal and sensitive) may revoke the consent at any time.

4.6. Regardless of the purpose, the owners of personal and/or sensitive data shall have facilitated access to the information on the treatment of their data, which must be made available in a clear, adequate and ostensible manner, indicating:

- a. specific purpose of the treatment;
- b. form and duration of the treatment, respecting trade and industry secrets;
- c. identification of the Manager;
- d. contact information of the Manager;
- e. information on shared use of data by the Manager and the purpose;
- f. responsibilities of the agents who will perform the treatment; and
- g. rights of the owner, explicitly mentioning their rights provided for in art. 18 of LGPD.

4.7. Termination of treatment of personal and sensitive data shall occur at the end of the contractual relation between the Manager and the client or when the investor does not hold any investment in the funds managed by the Manager, as the case may be, and the Manager may keep such personal and sensitive data even after termination of their treatment for the purposes of complying with legal or regulatory

obligations.

4.8. The Manager is responsible for guaranteeing the security of treated data, notwithstanding the Workers' training on that matter.

CHAPTER V

GENERAL PROVISIONS

5.1. This Policy must be construed by all Workers, jointly with the rules and procedures provided for in the Code of Ethics and Conduct of IG4 Capital Investimentos Ltda. and, as necessary, consulting the Department of Compliance of the Manager.

5.2. Any infraction or suspected infraction of this Policy must be reported to the Department of Compliance, through the Reporting Channel of IG4 Capital (<https://ig4capital.becompliance.com/compliance/canal-denuncias>) or by the e-mail compliance@ig4capital.com and must be dealt with according to the terms and penalties imposed by the Manager.