CONFIDENTIALITY POLICY, INFORMATION SECURITY, CYBER SECURITY AND LGPD

Updated Version: 2.0.0 - December/2023

CONFIDENTIALITY, INFORMATION SECURITY, CYBERSECURITY AND LGPD POLICY

Objective

To contribute to the improvement of the information and cyber security of DEZESSEIS DEZOITO GESTAO DE RECURSOS LTDA ("1618 INVESTIMENTOS"), with a view to guaranteeing the protection, maintenance of privacy, integrity, availability and confidentiality of the information it owns and/or holds, and establishing measures to be taken to identify and prevent contingencies that could jeopardize the performance of its activities.

Who does this apply to?

Partners, directors and employees who participate directly in the daily activities and business, representing 1618 INVESTIMENTOS (hereinafter, "Collaborators").

Review and Update

This Policy shall be reviewed and updated every two (2) years, or less if required by legal/ regulatory/self-regulatory changes.

Responsibilities

Employees must comply with the procedures set out in this Policy, reporting any irregularities to the Compliance and PLD Officer, who must assess them and submit them to the Compliance and Risk Committee, as appropriate. The Compliance and PLD Officer must ensure compliance with this Policy, and is responsible at 1618 INVESTIMENTOS for information security/ cybernetics, confidentiality and LGPD issues.

Operational and Business Context

This policy was drawn up taking into account the following assumptions and particularities of 1618 INVESTIMENTOS' operating and business model:

✓ All systems used by the manager, whether internal or third-party systems, are accessible via the web

✓ The suppliers of the systems used by 1618 INVESTIMENTOS are committed to availability, security and contingency plans compatible with the needs of 1618 INVESTIMENTOS;

1618 INVESTIMENTOS employees establish negotiations and formalize their understandings with clients through messaging tools and applications and/or corporate email;

The manager allocates funds through the use of investment brokers/platforms accessible via the WEB and available for any electronic device (laptops, smartphones, tablets or desktop computers);

✓ The portfolio consolidation system used by 1618 INVESTIMENTOS identifies clients by means of acronyms, eliminating the need to identify them by filling out a registration form with personal information;

- ✓ The portfolio consolidation system used by 1618 INVESTIMENTOS identifies clients using acronyms and does not require them to fill out a registration form with personal information;
- ✓ Files containing the personal and financial information of 1618 INVESTIMENTOS clients are stored in the cloud, with periodic backups of no more than 7 (seven) calendar days, and can be restored by requesting this information from the clients themselves;
- ✓ The electronic devices (laptops, smartphones, tablets) used to carry out 1618 INVESTIMENTOS' activities have access passwords and encryption;
- ✓ 1618 INVESTIMENTOS uses wireless networks to provide web access for its employees, service providers and visitors, all of which are duly protected by passwords. In the event of temporary unavailability of web access, Employees use redundant networks/routers;
- ✓ 1618 INVESTIMENTOS' physical space/office is the preferred location for its activities, meetings with clients, committees and commercial meetings with Employees or third parties. However, 1618 INVESTIMENTOS' activities, routines and systems are set up so that they can be carried out remotely.

Confidentiality Policy

"Confidential Information" is information that is not available to the public and which:

- ✓ Identify personal data or assets (of 1618 INVESTIMENTOS or its clients);
- ✓ Are the subject of a confidentiality agreement with third parties;
- ✓ Identify strategic actions - of the businesses of 1618 INVESTIMENTOS, its clients or the portfolios under management (1);
- ✓ All technical, legal and financial information, written or electronically filed, which relates to the activities of 1618 INVESTIMENTOS, and which is duly identified as being confidential, or which constitutes its intellectual or industrial property, and is not otherwise available to the general public;
- ✓ They are considered to be such due to a legal, regulatory and/or self-regulatory determination;
- ✓ and that Employees use to authenticate their identity (access passwords or badges), which are personal and non-transferable.

Disclosure of Confidential Information does not constitute non-compliance with this Policy: (i) with the prior authorization of the Compliance and PLD Officer, (ii) in compliance with orders from the Judiciary or competent regulatory, administrative or legislative authority, as well as (iii) when disclosure is justified, by virtue of the nature of the context of the disclosure of the information, to lawyers, auditors and counterparties.

In case of doubt, the Employee must first consult the Compliance and PLD Officer about the possibility of sharing Confidential Information.

Information Security Policy

The following principles guide information security at 1618 INVESTIMENTOS:

Confidentiality: access to information should be obtained only by authorized persons, and when

1 Whose disclosure may jeopardize the management of the businesses, clients and portfolios under the responsibility of 1618 INVESTIMENTOS, or reduce its competitive advantage.

is in fact necessary;
Availability: authorized persons must have access to the information whenever necessary;
Integrity: the information must be kept in its original state, in order to protect it, during storage or transmission, against undue alterations, whether intentional or accidental.
The following guidelines must be followed by all 1618 INVESTIMENTOS employees:

✓ Confidential information must be treated ethically and confidentially, and in accordance with the laws and internal regulations in force, avoiding misuse and undue exposure;
✓ Information should only be used for the purposes for which it was collected;
✓ Granting access to confidential information must comply with the criterion of least privilege, whereby users only have access to information resources that are essential for the full performance of their activities;
✓ The identification of any Collaborator must be unique, personal and non-transferable, qualifying them as responsible for the actions carried out;
✓ Segregation of common facilities, equipment and information, where applicable;
✓ The password is used as an electronic signature and must be kept secret and may not be shared.

Any risk or occurrence of a breach in the confidentiality and security of information must be reported to the Compliance and PLD Officer.

Controls and Obligations

Identification, Classification and Control of Information

Employees who receive or prepare information may, if necessary, classify it as "Confidential". To reach this conclusion, consideration must be given to issues of a legal and regulatory nature, business strategy, the risks of sharing, the need to restrict access and the impacts in the event of improper use of the information.

If there is information of a "Confidential" nature, access to it must be restricted and controlled.

Whenever necessary, information confidentiality agreements must be signed with third parties, under the supervision of the Compliance and PLD Director and, if deemed necessary, 1618 INVESTIMENTOS' legal counsel.

The information must be adequately protected. In case of doubt, the Employee should consult the Compliance and PLD Officer.

Disposal of Confidential Information stored on physical media should preferably be carried out using a paper shredder or incinerator.

Clean Table

No Confidential Information should be left in plain sight at Employees' workplaces, even when working remotely. In addition, when using a shared printer, the printed document must be collected immediately.

Access Management

The network, internet and e-mail services available at 1618 INVESTIMENTOS are its exclusive property, and moderate use for private purposes is permitted.
1618 INVESTIMENTOS may, at any time, with the prior approval of the Director of Compliance and PLD, and without obligation of prior notification:

- ✓ inspect the content and record the type of use made of e-mails by users;
- ✓ make these resources available to third parties, if deemed necessary;
- ✓ ask users to justify their use;
- ✓ monitor access to websites, applications, etc;
- ✓ blocking access to websites.

In the event of a change of area or dismissal of the Employee, the respective access password is cancelled, in order to prevent unauthorized access by the former Employee.

The equipment, tools and systems provided to Employees must be configured with the necessary controls to comply with the security requirements applicable to 1618 INVESTIMENTOS.

Only duly authorized Employees will have access (2) to the premises and systems to which they are granted access, as well as to files, directories and/or folders on the 1618 INVESTIMENTOS network, through physical and logical segregation.

Risk Management, Information Security Incident Handling, Business Continuity and Backups

Information security risks and incidents must be reported to the Compliance and PLD Director, who will adopt the appropriate measures.

The contingency and continuity plan for the main systems and services provided by third parties must be tested in order to reduce the risk of loss of confidentiality, integrity and availability of information assets. The Compliance and PLD Officer must request the results of these tests from the suppliers of these systems, as well as monitor the solution of any deficiencies identified in these tests.

In the event of information leakage or improper access to information, the Compliance and PLD Officer must be immediately notified so that the appropriate measures can be taken(3).

Cybersecurity Policy

The main threats and risks to 1618 INVESTIMENTOS' cyber assets are:

- ✓ Malware - software designed to corrupt computers and networks, such as:

- ✓ viruses: software that causes damage to machines, networks, software and databases;
- ✓ Trojan horses: appear inside other software, creating a way into the machine;
- ✓ spyware: malicious software that collects and monitors the activities of hacked machines;

2 Any exceptions must be requested in advance from the Compliance and PLD Officer.

3 This may range from a simple reprimand for access, or a message to the wrong recipient of the message sent (so that they can delete its content once and for all), to the study and effective implementation of legal measures, when and if appropriate, without prejudice to the investigation and possible punishment of the Collaborators involved.

- ✓ ransomware: malicious software that blocks access to systems and databases, demanding ransoms to restore use/access.

- Social engineering - manipulation methods to obtain confidential information, such as passwords, personal data and credit card numbers, for example:
  - ✓ pharming: directs the user to a fraudulent website without their knowledge;
  - ✓ phishing: links transmitted by e-mails simulating trustworthy people or companies sending apparently official electronic communication in order to obtain confidential information;
  - ✓ vishing: impersonating trustworthy people or companies in order to obtain confidential information through telephone calls;
  - ✓ smishing: impersonating trusted people or companies in order to obtain confidential information via text messages;
  - ✓ DDOS (distributed denial of services) attacks and botnets - attacks aimed at denying or delaying access to the institution's services or systems;
  - ✓ advanced persistent threats - attacks carried out by sophisticated attackers using knowledge and tools to detect and exploit specific weaknesses in a technological environment.

Controls and Obligations

In providing its services, 1618 INVESTIMENTOS obtains and handles sensitive information that is not available to the general public, and which could cause irreparable losses in the event of misuse, negligence or leaks (4).
The Compliance and PLD Officer is responsible for these issues at 1618 INVESTIMENTOS.
These are mandatory cybersecurity items (company):

o Adequate protection of 1618 INVESTIMENTOS' cyber assets, including its network, systems, software, websites, equipment and electronic files.
o Restricting and controlling access and privileges for users who are not 1618 INVESTIMENTOS employees;
o Invalidating the accounts of employees and service providers when they leave the company;
o When necessary, block user access keys and, when necessary, carry out audits to check for undue access;
o Delete or disable inactive accounts;
o Provide privileged account passwords only to Employees who actually need such privileges, keeping proper records and controls;
o Ensure compliance with the backup procedure for 1618 INVESTIMENTOS' servers and cyber, electronic and computer assets;
o Detect, identify, record and report violations or unauthorized access attempts to the Compliance and PLD Director;
o Organize training related to the security of information assets whenever necessary;
o In cases where the above services and controls are outsourced, the contractual conditions must guarantee that the service provider attests to this protection;

4 The potential risks relating to such data involve intrusions, erroneous or malicious dissemination, improper access and/or its theft/ misappropriation.

o If necessary, based on the results of adherence tests, review these practices;
o 1618 INVESTIMENTOS has server security for access to its network, in order to keep the work environment available and free from viruses and unwanted access. The system for preventing virus attacks is regularly updated;
o Files are systematically backed up. Updated backup data is stored in a secure, monitored location.

These are MANDATORY cybersecurity items (Employees):

o Only send messages to the people involved in the subject matter, making sure the destination addresses are correct;
o Only print messages when really necessary;
o If you spot a message with a suspicious title or attachment, make sure it is safe to open, to avoid viruses or malicious codes;
o In the event of receiving messages that contravene the rules established by 1618 INVESTIMENTOS, NEVER pass them on, alerting the person in charge of your area and the Compliance and PLD Director, if applicable;
o When absent from your workplace, even when working remotely and even temporarily, lock your workstation;
o When going on vacation or being away for extended periods, the Employee must use the temporary e-mail absence feature;
o Use equipment, applications, printers, access to websites and e-mail (and other technological tools) for the primary purpose of serving the interests of 1618 INVESTIMENTOS5;
o Technologies, brands, methodologies and any information belonging to 1618 INVESTIMENTOS must not be used for private purposes, nor passed on to others, even if they have been obtained or developed by the Collaborator in his/her work environment;
o Each Employee will only have access to electronic folders related to their area and to folders common to all Employees.

These are FORBIDDEN cybersecurity items (Collaborators):

o Sending e-mails or accessing websites that promote the dissemination of messages, products, images or information that interfere with the performance of professional activities (6);
o Exchanging information that causes a breach of banking secrecy and/or is of a confidential or strategic nature (7);
o Intentionally harming Internet users by developing programs, unauthorized access to computers and altering files, programs and data on the 1618 INVESTIMENTOS network;
o Disseminate propaganda or advertise particular products or services through 1618 INVESTIMENTOS' electronic mail;
o Changing any technical configuration of the software that compromises the level of security,

5 Computers, files and corporate e-mail archives may be inspected, regardless of prior notification to the Employee, in order to detect erroneous or malicious dissemination, improper access and/or theft/ misappropriation of information.
6 In particular, pornographic, racist or offensive to morals and ethical principles content is prohibited.
7 With the exception, of course, of information flows necessary for the management of funds and portfolios with institutions involved in client operations.

or prevent/difficulty its monitoring by the Compliance and PLD Officer;
o Hiring access providers without the prior authorization or knowledge of the Compliance and PLD Officer;
o Use of information sharers, such as Peer-to-Peer networks (P2P - e.g. Kazaa, eDonkey, eMule, BitTorrent and similar) on 1618 INVESTIMENTOS premises.

Exceptions to this Cybersecurity Policy (Employees):

o In the event of the use of equipment or electronic devices owned by employees to carry out their activities at 1618 INVESTIMENTOS, they undertake to adopt the aforementioned security measures in order to preserve their equipment and minimize the risk of compromising the security of sensitive information belonging to 1618 INVESTIMENTOS, its clients and business partners, and may use such equipment for the various purposes they deem pertinent;
o The Compliance and PLD Director may authorize exceptions to this policy, which must be formalized by e-mail.

Personal Data Protection Policy (LGPD)

1618 INVESTIMENTOS, in the exercise of its activities, has and/or may have access to personal data, as defined in Law No. 13,709, of August 14, 2018 ("LGPD").
The processing of such data is carried out within the strict limits and purposes of the law and applicable regulations (especially, without limitation, CVM rules relating to registration and identification of clients and operations), given that the access referred to herein is a mandatory condition for the performance of 1618 INVESTIMENTOS' activities with the investing public: thus, its access and processing is carried out in accordance with the structure, scale and volume of operations of 1618 INVESTIMENTOS, as well as the sensitivity of the data processed.
Personal data is therefore collected and stored solely and only for strict compliance with the legislation and regulations applicable to 1618 INVESTIMENTOS' activities, and it is absolutely forbidden for 1618 INVESTIMENTOS and/or any of its Collaborators to use it in any other way: any use shared with regulators and authorities may only be carried out under the strict terms and limits of the current rules applicable to 1618 INVESTIMENTOS, and for strict compliance with them.
The processing and storage of the personal data received will last for the duration of the relationship between 1618 INVESTIMENTOS and the holder(s) of the personal data, always simultaneously respecting the period determined by the rules in force applicable to them.
1618 INVESTIMENTOS' contact information and responsible parties in this regard can be found on its website, and it is the responsibility of the Compliance and PLD Director to supervise Employees and ensure the processing of such data, always safeguarding the rights of the data subject contemplated in art. 18 of the LGPD, which are:

- ✓ Confirmation to the data subject of the existence of the processing of their personal data;
- ✓ access to your data held by 1618 INVESTIMENTOS;
- ✓ correction of incomplete, inaccurate or outdated data;
- ✓ anonymization, blocking or deletion of data that is unnecessary, excessive or processed in breach of the provisions of the LGPD;

- ✓ portability of the data to another service or product provider, upon express request, in accordance with the regulations of the national authority, observing commercial and industrial secrets;
- ✓ deletion of personal data processed with the consent of the data subject (except, under the terms of art. 16 of the LGPD, in the event of (a) compliance with a legal or regulatory obligation by 1618 INVESTIMENTOS, (b) transfer to a third party, provided that the data processing requirements set out in the LGPD are respected, or (c) exclusive use by 1618 INVESTIMENTOS, with access by a third party prohibited, and provided that the data is anonymized);
- ✓ information on the public and private entities with which the controller has shared data;
- ✓ information on the possibility of not providing consent and the consequences of refusing to do so;
- ✓ revocation of consent.

In the event that consent for the processing of personal data is required, if there are changes in the purpose for processing personal data that are not compatible with the original consent, 1618 INVESTIMENTOS shall inform the data subject in advance of the changes in purpose, and the data subject may revoke the consent if he/she disagrees with the changes.
The processing of personal data will cease in the following cases:

- ✓ verification that the purpose has been achieved or that the data are no longer necessary or relevant to the achievement of the specific purpose pursued;
- ✓ ✓ end of the processing period;
- ✓ ✓ communication from the data subject, including when exercising their right to withdraw consent; or
- ✓ ✓ determination by the national authority, when there has been a violation of the provisions of the LGPD.

Control Adherence Tests

The effectiveness of these Policies is verified through periodic tests of the existing controls, at intervals of no more than one (1) year, under the responsibility of the Compliance and PLD Officer and reported to the Compliance and Risk Committee.
The tests (8) must verify that:

- ✓ Human and computer resources are adequate for the size of the company and the areas in which it operates;
- ✓ There is an adequate level of confidentiality and access to confidential information, with identification of the people who have access to this information;
- ✓ ✓ There is physical and logical segregation;
- ✓ ✓ Computer resources and physical and logical access control are protected;
- ✓ ✓ Records are kept so that audits and inspections can be carried out, as well as compliance with LGPD obligations.

8 Which may be carried out by third parties, or the subject of a contractual obligation, subject to reporting by service providers, data providers, applications and tools/software. Such content may be included in the annual compliance report required by the applicable CVM regulations.