INFORMATION SECURITY AND ASSET MANAGEMENT POLICY

1. Introduction - Information Security and Asset Management Policy

1.1. Objective

1.1.1. This Information Security and Asset Management Policy ("Policy") is intended to establish guidelines and standards on information security and management of /asbz information assets, in addition to defining the roles and responsibilities of its employees, third parties and service providers, with a view to protecting the information of /asbz, its clients and the general public.

1.1.2. This Policy should be read in conjunction with the additional rules below, and in the event of a discrepancy between any of them and this Policy, the provisions with more specific content will prevail.

- Code of Conduct and Ethics
- Business Continuity Plan
- Website Privacy Policy

1.2. Concept

1.2.1. Information is an asset that has great value for /asbz, and must be properly used and protected by its employees, business partners and service providers. The adoption of policies, rules and procedures aimed at guaranteeing the security of corporate information must be a constant priority of the organization, so that the risk of failures, damages and/or losses that may compromise the image and objectives of /asbz may be reduced.

1.2.2. Information can be manipulated in several ways: through electronic files, the Internet, databases, electronic messages, in print, verbally, on removable media, and among other means present in our daily lives, such as the use of cell phones, corporate and/or personal notebooks**;**

1.2.3. Information security is characterized here by the preservation of the following principles:

1.2.3.1. **Confidentiality**: Guarantee that access to information is obtained and granted only by authorized persons;

1.2.3.2. **Availability:** Assurance that employees, third parties and authorized service providers obtain access to information (and corresponding assets) whenever necessary, limited to what is in fact essential for the purpose in question; and

1.2.3.3. **Integrity**: Guarantee that the information is kept in its original condition, aiming to protect it, while having its custody or transmiting it, against any undue, intentional or accidental alterations; that is, only changes, deletions, and additions authorized by /asbz should be made to the information.

1.2.4. To ensure these concepts, information must be properly managed and protected against fraud, espionage, unintentional loss, accidents and other threats arising from weaknesses in systems, processes and people.

1.3. Applicability

1.3.1. It applies to all permanent or temporary employees, as well as third parties and service providers, who access information belonging to /asbz, who must read, understand, and act in accordance with the terms and conditions of this Policy.

1.3.2. The Policy also applies to all locations from which /asbz systems can be accessed (including home use). Third parties who have access to /asbz systems, through links, must demonstrate that they have an information security policy in place that complies with the security requirements adopted by /asbz. A copy of any third party security policy will be maintained with the contract or agreement entered into with them.

1.3.3. Each and every User of computerized resources of /asbz has a responsibility to protect the security and integrity of information and IT equipment.

1.4. Policy

1.4.1. /asbz undertakes to:

- Protect the confidentiality, integrity and availability of any data it holds on its systems. This includes protecting any device owned by /asbz that may transport or access data, as well as protecting hard copies of the data on paper whenever possible (for example, rules on handling, storing, and disposing of documents);
- Comply with legal and contractual obligations;
- Protect /asbz's intellectual property rights;
- Produce, maintain and test business continuity plans;
- Prohibit the unauthorized use of /asbz information and systems;
- Communicate and disseminate this Policy to all persons who process data in the office;

- Provide training on information security and Personal Data protection to the employees at the firm; and
- Conduct internally, in a proper manner, all procedures to remedy any actual or suspected information security violations, and, when necessary, report them to the competent bodies, including, without limitation, the Brazilian Data Protection Authority ("ANPD").

1.5. Risk assessment and information classification

1.5.1. The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security is therefore a risk assessment process in order to identify and classify the character of the information held, the adverse consequences of security breaches, and the likelihood of those consequences occurring;

1.5.2. The risk assessment should identify /asbz information assets; define ownership of these assets; and classify them according to their sensitivity and/or criticality to /asbz as a whole. While assessing risk, /asbz must consider the asset's value, threats to that asset, and its vulnerability;

1.5.3. Where appropriate, information assets should be labeled and handled according to criticality and sensitivity;

1.5.4. Information security risk assessments should be periodically reviewed and performed as necessary during the delivery and operational maintenance of /asbz infrastructure, systems and processes;

1.5.5. Personal Data must be processed in accordance with the provisions of the LGPD, any guidelines from relevant authorities, including, without limitation, the ANPD, and in accordance with this Policy;

1.5.6. LGPD requires that appropriate technical and organizational steps be taken against unauthorized or illegal processing of Personal Data, as well as against accidental loss/destruction or damage to Personal Data; and

1.5.7. A higher level of security must be provided, where necessary, for the so-called sensitive and minors' Personal Data, defined by the LGPD as those related to racial or ethnic origin, religious belief, political opinion, union affiliation or religious, philosophical or political organization membership, data relating to health or sex life, and genetic or biometric data when linked to a natural person.

2. Glossary

2.1. Information Security

2.1.1. According to the context of this Policy, Information Security consists of the set of guidelines and good practices related to the use and confidentiality of information, Personal Data and processes under the management of any and all employees, third parties and service providers. That is, it refers to all documents, standards or manuals that determine actions to ensure information security.

2.2. Information Asset

2.2.1. An information asset is any element that supports one or more business processes of a business unit or area, that is, everything that has value for the firm. ISO 27001 requires that all relevant assets be identified and inventoried. When it comes to information security, "asset inventory" should be understood as a broader set of assets, which includes systems, people, physical environments, among others.

2.2.2. Below are some examples of assets:

Users	Computers	Disks
Printers	Mobile media	Systems
Database	Servers	Network switches
Links	Documents	Agreements
Contracts	Scanners	Administrators

2.3. Threat

2.3.1. A potential cause of an incident that may harm /asbz.

2.4. Information Security Incident

2.4.1. Any adverse event, confirmed or suspected, related to the security of information systems, which accidentally or illegally causes the destruction, loss, alteration, unauthorized access or acquisition, disclosure, misuse or access to information and Personal Data not encrypted, transmitted, stored or otherwise processed by /asbz.

2.5. Users

2.5.1. Lawyers, interns, apprentices, workers with an employment relationship, from any area, or third parties allocated in the provision of services, irrespective of the legal rules to which they are subject, as well as other individuals, employees, or organizations duly authorized to use or manipulate any information asset of /asbz while performing their professional activities.

2.6. Personal Data

2.6.1. Any and all information concerning an identified or identifiable individual, including, but not limited to, name, identification documents, telephone numbers, email addresses, mailing address, bank and financial details, date of birth, gender, parents' names, demographic information, etc..

2.7. Confidential Information

2.7.1. Includes, but is not limited to, information – stored in any form – related to /asbz and its business, information related to clients or potential clients, information subject to a disclosure restriction, information subject to proprietary right or trade secret, information that is not readily available to the public, and any and all information that an /asbz employee knows or should know would be considered sensitive by /asbz, its clients and potential clients as confidential materials. Examples include: documents, contracts, graphics, images, drawings, designs, know-how, trade secrets, commercial, technical, administrative, strategic, marketing, financial information and other data.

2.7.2. If the User has doubts when assessing whether or not a piece of information or data is confidential, he/she must treat it as confidential.

2.8. Data Processing Officer (DPO)

2.8.1. Team or individual within /asbz responsible for acting as a communication channel between the firm, the Personal Data subjects and the ANPD. In addition, the DPO is responsible for assisting the firm in complying with its legal obligations regarding privacy and protection of Personal Data.

2.9. Brazilian Data Protection Authority (ANPD)

2.9.1. Government agency responsible for ensuring, implementing and monitoring compliance with the Data Privacy Law throughout the Brazilian territory.

3. Roles and responsibilities

3.1. Information Security Working Group

3.1.1. The Information Security Working Group is hereby created - the members of which are to be appointed by the /asbz Director of Innovation - to act whenever deemed necessary;

3.1.2. The Group will be responsible for analyzing, reviewing and proposing the approval of policies and standards related to information security and the management of /asbz assets; and, furthermore, the Group will also:

3.1.3. Ensure the availability of the necessary resources for an effective management of Information Security and assets;

3.1.4. Ensure that information security activities are performed in compliance with this Policy;

3.1.5. Promote the dissemination of the Policy and take the necessary actions to propagate a culture of information security and protection of Personal Data in the /asbz environment;

3.1.6. Analyze and investigate incidents related to the Policy; and

3.1.7. Decide on the application of sanctions to incidents identified and analyzed.

3.2. Information Technology (IT) Department

The Information Technology Department will be responsible for:

3.2.1. Supporting the /asbz Information Security Working Group in its decisions;

3.2.2. Conducting the management and operation of Information Security, as well as the management of assets, based on this Policy and other rules and procedures of /asbz;

3.2.3. Providing all management information concerning Information Security and, when applicable, assets, as may be requested by the Information Security Working Group or by the Executive Board;

3.2.4. Preparing and proposing to the /asbz Information Security Working Group the rules and procedures for information security and asset management, as necessary to enforce the Policy;

3.2.5. Before granting access to /asbz information, requiring the execution of a confidentiality agreement from Users who are not covered by an existing contract or legal or regulatory obligation, for example, during the survey phase for submission of business proposals;

3.2.6. Identifying and assessing the main threats to information security, as well as proposing and, when approved, implementing corrective measures to reduce the risk;

3.2.7. Taking appropriate actions to enforce the terms of this Policy;

3.2.8. Managing information security incidents, ensuring adequate treatment of the cases identified;

3.2.9. Ensuring that information security activities are carried out in accordance with this Policy; and

3.2.10. Conducting training for Users and taking other appropriate measures for the dissemination of this Policy and assimilation of all its concepts and user obligations.

3.3. Users

Users are responsible for:

3.3.1. Reading, understanding and fully complying with the terms of the Policy, as well as other applicable rules and procedures;

3.3.2. Forwarding any questions and/or requests for clarification about the Policy, its rules and procedures to the /asbz Information Security Working Group;

3.3.3. Communicating to /asbz's Director of Innovation any event that violates this Policy or puts/may put the security of /asbz's information, computing resources and assets at risk;

3.3.4. Participating in all training provided by the Information Security regarding Information Security; and

3.3.5. Responding for non-compliance with the Security Policy, standards and procedures, as defined in the sanctions and punishments section.

4. General Guidelines

4.1. General Aspects

4.1.1. This Policy is an integral part of the verbal or tacit, written or express employment contract of the Users, for all legal purposes, together with the admission kit provided by the People Management department;

4.1.2. This Policy informs each user that the /asbz environments, systems, devices, servers and networks may be monitored and recorded, and that the records thus obtained may be used to detect violations of this Policy and of other standards of

information security, which may serve as evidence for the application of disciplinary measures, administrative and/or judicial proceedings;

4.1.3. An engaged and proactive attitude with regard to the protection of /asbz information must be a constant priority for all Users and business areas, thus reducing the risk of failures, damages and/or or losses that could compromise the firm's image and goals;

4.1.4. Corporate information must be handled in accordance with current laws and internal regulations and used only for the purpose for which it was collected, avoiding misuse and/or improper exposure thereof; and

4.1.5. Users are prohibited from using company data for unlawful purposes, which may include the violation of any law, regulation or rules.

4.2. Access to Information and information systems

4.2.1. The information (in physical or logical format) and the corporate technological environments used by the Users are the exclusive property of /asbz, and cannot be interpreted as for personal use;

4.2.2. Access to /asbz information must be restricted to authorized Users and must be protected by appropriate practical physical and/or logical controls;

4.2.3. Access permissions to /asbz systems and platforms will be granted by the Information Technology Department;

4.2.4. Access permissions for Users who, for the performance of their activities, need access to /asbz systems, must be granted only during the term of their contract;

4.2.5. Access to physical information assets – for example, printed paper documents and media containing information – will be governed by the principles stated above, as applicable;

4.2.6. Proper procedures must be in place to ensure that all Users have information and physical access permissions granted quickly when joining /asbz, revoked when leaving the organization, and updated when their role changes. Those who are dismissed or have their contract terminated will also be required to return all /asbz assets that are in their possession after their contract is terminated;

4.2.7. Domain administrator privileges – those that are able to override the system and application controls on multiple devices across /asbz – should be restricted to those authorized to perform systems administration only. Such privileges must be authorized by the Information Technology Department, once appropriate risk assessments have been reviewed and made as to the validity of requirements and the skill levels of those requesting increased privileges;

4.2.8. All suppliers or contractors who process /asbz information must provide /asbz with guarantees that they have controls compatible with the precepts of the LGPD, as well as those adopted by /asbz itself; and

4.2.9. In cases where the data processed by the supplier or contractor are sensitive (as defined by the LGPD), a third-party security assessment (vendor assessment) must be completed by the supplier.

4.3. Use of removable storage devices and personal computer equipment

4.3.1. /asbz acknowledges that there may be occasions when Users need to use removable storage devices provided by /asbz to access information (including Personal Data). /asbz must ensure that all devices provided are fully encrypted and that Users are aware of this policy;

4.3.2. /asbz acknowledges that there may be occasions when Users need to use their own device to access information (including Personal Data and emails). Users must ensure that such devices are protected by appropriate authentication factors and antivirus. The Information Technology Department or the /asbz Director of Innovation may revoke access to /asbz systems or information on personal devices where the data contained/transmitted is considered sensitive and the personal device is not suitable.

4.3.3. Users acknowledge that:

- Privately owned computing equipment used to access /asbz information or connect to the /asbz network must be password protected, have up-to-date antivirus installed, as well as all relevant operating system updates and all third-party programs that the Information Technology Department deems necessary;
- Use of personal devices to access email is permitted. It is recommended that Users seek guidance from the Information Technology Department to ensure that the configuration of email connections is secure, devices are secured with key/password/biometrics lock and, where appropriate or feasible, device encryption; and
- /asbz reserves the right to stop transmitting or accessing any of the data it holds if this Policy is not followed.

4.3.4. /asbz reserves the right to disconnect the device from its corporate network and disable its services without prior notification, in case of any security incident (virus, data breach, among others) or in case of violation of this Policy and other information security rules or in certain situations as decided by the Director of Innovation of /asbz; and

4.3.5. In the case of information security incidents involving devices that contain /asbz information assets, Users must immediately report such incident through the email of the Innovation Director of / asbz and incidents@asbz.com.br.

4.4. Monitoring computers, e-mail and Internet

4.4.1. Email from /asbz Users is not routinely read or monitored. However, to ensure the security, confidentiality, availability and integrity of /asbz's IT systems and assets, under certain circumstances, in order to investigate fraud situations and information security incidents, authorized members of the Information Technology Department or other authorized personnel may access /asbz computers, emails and internet systems – including online digital platforms such as the cloud or other recording, database and backup systems; and

4.4.2. /asbz may investigate violations of the law or internal rules and policies of the company itself, which may involve access to the employee's computer and electronic records. Such an investigation may occur upon suspicion of misconduct or gross negligence by the employee, and will be conducted in accordance with the provisions of the Code of Ethics and Conduct.

4.5. Monitoring by security cameras

4.5.1. To reinforce the security of its employees and visitors to its facilities, /asbz operates security cameras in all its premises. The surveillance system is continuous and permanent;

4.5.2. The cameras are not used for surveillance of specific people, but the recorded images can be accessed and used for monitoring activities related to /asbz, including as support in internal investigations or investigations promoted by the relevant authorities; and

4.5.3. Cameras in general, including those built in cell phones, must not be used to record images of /asbz or any individual's operations without their prior consent.

4.6. Clear desk / Screen policy

4.6.1. Outside normal working hours, all confidential information, whether marked as such or not, must be protected; this can include keeping it inside a locked cabinet or on a desk with locked drawers. During normal business hours, this information must be hidden or protected if the desks are left unattended or in the case of an open space environment;

4.6.2. Confidential printed information that will be disposed of in a timely manner must be placed in a dedicated disposal compartment for confidential materials as soon as possible, or kept securely protected until the time of disposal;

4.6.3. Documents must be removed immediately from printers and photocopiers after use;

4.6.4. Desktop computers should be automatically disconnected or locked after 5 minutes of inactivity (unless it is necessary to remain on for operational purposes), to ensure that standalone computer systems do not become a potential means of gaining unauthorized access to the network;

4.6.5. Those who are responsible for meetings must ensure that no confidential information is left in the room at the end of the meeting, even documents thrown in wastebaskets; and

4.6.6. /asbz shall ensure that Users have adequate and sufficient storage facilities to enable them to comply with this Policy.

4.7. Security of physical media

4.7.1. Those responsible for the information must ensure that any physical media (for example, paper, CD-ROMs, hard drives) used to store information containing Personal Data are protected in order to prevent unauthorized access by third parties;

4.7.2. The physical security of such information should be in the form of lockable cabinets or other not easily transportable containers, with keys or combination codes accessible only to authorized persons. When lockers or storage compartments are not lockable, they must be located in a room whose access is restricted to authorized personnel only; and

4.7.3. When physical media is in an environment (or room) in which it is not possible to store it in a locked location, the environment (or room) itself must be locked when not in use (see also 4.6.1 above).

4.8. Retention and disposal of information

4.8.1. /asbz, through its internal areas, must always seek the processing of Personal Data strictly necessary to meet the intended purpose, without excessive data collection;

4.8.2. The information must be kept only for the time necessary to fulfill its intended purpose;

4.8.3. Users are not allowed to store personal photos, files or movies on the disk of /asbz machines, so as to avoid consuming storage units with data not aligned with the business. If these types of files are found by the Information Technology Department, they may be deleted without prior notice to Users;

4.8.4. In case of doubt about the storage period of certain information, Users must consult the specific rule that defines the type of information that must be kept by the respective areas, together with the retention periods; and

4.8.5. In case of any sign of unusual situation or suspicion of security breach related to the storage of data, Users must immediately report the event through the email of the Director of Innovation of /asbz and incidents@asbz.com.br.

4.9. Electronic mail

4.9.1. /asbz provides the use of an electronic mail system as an essential tool for Users to use it for exclusively professional purposes;

4.9.2. No User should send messages that could be interpreted as offensive, by any other person, be it a legal entity or an invidual;

4.9.3. No User shall transmit or retransmit messages that violate the provisions of the /asbz Code of Ethics and Conduct.

4.9.4. Users should not participate in “chain letters” of any nature, direct mail, signature campaigns, etc.; and

4.9.5. Users must act with care and attention while opening electronic mail items, and must immediately report any suspicion of spam, phishing and the like to the Information Technology Department and the Data Processing Officer of the firm, so that, together, they can evaluate the necessary steps to be taken.

4.10. Internet

4.10.1. /asbz provides Internet access as an essential tool for Users to use it for exclusively professional purposes; and

4.10.2. No User may use the Internet in a way that violates the provisions of the /asbz Code of Ethics and Conduct.

4.11. Identification

4.11.1. Identification devices and passwords protect the identity of Users, preventing a person from impersonating another person before /asbz and/or third parties;

4.11.2. All identification devices used by /asbz, such as the User's registration number, badge, system access identifications, digital certificates and signatures and biometric data must be associated with a individual and unequivocally linked to their official documents recognized by Brazilian legislation;

4.11.3. Accordingly, no personal identification devices may be shared with other people under any circumstances. The use of another person's identification devices and/or passwords constitutes a crime provided in the Brazilian Penal Code (art. 307 - false identity);

4.11.4. Users must necessarily have a variable-length password, with at least 8 (eight) alphanumeric characters, using special characters (@ # $ %) and variation between upper and lowercase;

4.11.5. Each User is responsible for memorizing their own password, as well as protecting and guarding the identification devices assigned to them;

4.11.6. Passwords must not be written down or stored in electronic files (Word, Excel, Notepad, etc.) understandable by human language (unencrypted) or in browsers. They should not be based on personal information, such as your own name, a family member's name, date of birth, address, vehicle license plate, company name, department name, and should not consist of obvious keyboard combinations, among others;

4.11.7. After 3 (three) failed attempts to access the user's account it will be blocked. To unlock it, the user must contact the Information Technology Department at /asbz, and start a password renewal process;

4.11.8. Temporary passwords provided by the Information Technology Department must be replaced by permanent personal passwords immediately;

4.11.9. Users can change their own password, and should be instructed to do so, if they suspect that third parties have obtained undue access to their access credentials; and

4.11.10. Passwords must be changed every 90 (ninety) days, and the last 3 (three) passwords cannot be repeated. Systems must force passwords to be changed within this maximum timeframe.

4.12. Sharing and disclosing information

4.12.1. Whenever necessary, the sharing of information, especially that containing Personal Data and confidential information, either between /asbz's internal areas or with third parties - such as customers, carriers and service providers - must take place through secure, available means validated by /asbz for this purpose. The use of WhatsApp, Telegram or similar means that are not properly secured should be avoided.

4.13. Copyrights and third parties' rights

4.13.1. Users are not allowed to install, use or copy any piece of software unless expressly permitted by the lawful copyright holder thereof and/or the Information Technology Department;

4.13.2. The use of information assets to store, transmit or disseminate books, music, videos or any other files that are protected by copyright shall be forbidden unless the proper permission of the author is obtained, or if the situation appears among the limitations of copyright provided for in art. 46 of the Copyright Law; and

4.13.3. Any User who becomes aware of any unauthorized reproduction of software, books, videos, or any other similar material within /asbz must immediately notify the Information Technology Department.

4.14. Ethics and Conduct

4.12.1 Users at /asbz must follow the guidelines of the /asbz Code of Ethics and Conduct. They must also act responsibly on social media, especially those of a professional nature, of which they are a part, forbidding the publication of content with disrespectful, discriminatory approach or that may generate an unfavorable view, both to the individual and to /asbz. Users may not post images or comments that may reveal Confidential Information of /asbz or clients and must abastain from making judgments about /asbz, partners, clients, competitors or co-workers.

4.15. Audit Process

4.15.1. /asbz reserves the right to carry out internal or external audit processes at any time and without prior notice to Users.

4.16. External parties

4.16.1. The service provision contracts entered into by /asbz, in which the contractors will have access to information, systems and/or the technological environment of /asbz, must contain clauses that (i) guarantee the confidentiality between the parties, (ii) provide for the protection and privacy of the Personal Data involved, (iii) establish liability limits in case of misuse of such data, and (iv) ensure, at a minimum, that the professionals under their responsibility comply with this Policy and other /asbz Information Security standards, following the guidelines of /asbz's Code of Ethics and Conduct.

5. Unforeseen Cases

5.1. Unforeseen cases will be evaluated by the Information Security Working Group for further deliberation;

5.2. The guidelines established in this Policy and in other security rules and procedures are not limited in view of the continuous technological evolution and constant emergence of new threats. Therefore, they are not an exhaustive list, as it is the obligation of the User of the /asbz information to adopt, whenever possible, other security measures in addition to those provided herein, in order to guarantee the protection of the /asbz information; and

5.3. Unforeseen cases must also be formally reported to the e-mail address of the Innovation Director at /asbz and to incidents@asbz.com.br.

6. Reviews

6.1.1. This standard is revised annually or as determined by the Information Security Working Group.

Date	Edition	Approved by
01.04.2022	1	Institutional Management Committee and Executive Board

(* * *)