INFORMATION SECURITY POLICY[1]

1. GOAL

The objective of this policy is to establish concepts, principles and guidelines for information security and disseminate them to all involved, in order to bring improvements in the quality of services provided by the company and strengthen the security culture and to protect the information treated in Méliuz's environment, which may affect the continuity of the business, cause financial losses, non-compliance with legislation or bring about negative impacts on the company's image, if compromised, altered, destroyed or disclosed in an unauthorized or unplanned manner.

2. SCOPE

The Information Security Policy applies to all employees, customers and partners and service providers, including third-party service providers who use the processing environment or access the information belonging to Méliuz or of its responsibility.

3. PRINCIPLES OF INFORMATION SECURITY

Méliuz, aiming at the proper treatment of the information related to the company and to all its customers, partners, employees or of any other information relevant to those involved (*Informed in the coverage section)*, is based on the following principles of information security:

I. **Confidentiality**: Any access to the information should be obtained only by authorized persons, and only when it is necessary;
II. **Availability**: The information must be available for access, whenever necessary;
III. **Integrity**: The accuracy and completeness of the information and methods of its processing should be ensured, as well as transparency in dealing with the stakeholders involved.

To comply with these principles, we have established processes and internal controls of information security, aiming at the protection of data throughout its life cycle (creation, handling, storage, transportation, and disposal):

1. Ensure the protection of information against undue access, copying, modification, destruction or unauthorized disclosure;
2. Ensure the principle of transparency, where the purpose of the use of information must be explained, and must be used only for this purpose;
3. Ensure due treatment of security incidents, considering the detection, mitigation and analysis of root cause;
4. Ensure the prevention, detection, and mitigation of incidents related to Méliuz's environment that store or process information, reducing its vulnerabilities;
5. Establish periodic tests of business continuity, considering established incident scenarios;
6. Protect assets through procedures for monitoring the networks and technological resources of the company and its employees in order to detect and prevent attacks and intrusions;
7. Inform customers and users about the information security measures necessary for the use and processing of information;
8. Ensure compliance with policies, standards and requirements of information security in the company;
9. Raise awareness, educate, evaluate and disseminate the culture of information security to all employees and third parties, aiming at full compliance with safety principles and guidelines.

4. Communication channels with information security

In case of questions regarding this policy or other procedures related to information security, as well as incidents, infractions, or related suspicions, please contact the security department, through our digital service channel, available on our official website.

[1] Version 01 - Last updated on 02/16/2022