

Information Security Policy

Information Security Policy

Information and information systems' protection have strategic significance for the company to achieve its short and long-term objectives.

The Management acknowledging the information and information systems' importance in business processes implementation, supports and promotes actions aiming to safeguard the systems' normal operation. The Company has established an Information Security Policy aiming to:

- Ensure the confidentiality, availability, and integrity of the information it processes
- Protect the data subjects' rights within the scope of its business operations
- Comply with the applicable legislative and regulatory requirements
- Promptly address incidents that may violate the Information Security

For this reason, the company takes the proper technical and organizational measures to ensure the availability, integrity, and confidentiality of the data it process. At the same time, it adheres to policies and procedures in the context of which the following are defined:

- Organizational units and roles required for Information Security issues monitoring
- Technical measures for controlling and restricting access to information and information systems
- Information classification method based on its importance and criticality
- The required actions for information protection during the phases of processing, storing and transferring
- Methods for training the company's employees and partners in Information Security
- Information Security incidents handling method
- Methods for ensuring the continuous operation of business processes in cases of information systems failures or physical disasters

The company conducts periodically Information Security risk assessments and determines the required corrective actions. It evaluates the effectiveness of the Information Security procedures by defining performance indicators, describing their measurement methods, producing and reviewing periodic reports with a view to continuously improving the system.



AUTO BANK

The Information Security Officer is responsible for the Information Security Management System operation and control as well as for taking the required initiatives to eliminate any factor that may lead to company's information availability, integrity, or confidentiality compromise.

Company's employees and partners with access to information and information systems are responsible for adhering to the rules of the implemented Information Security Policy.