



INFORMATION SECURITY POLICY

The information's confidentiality, integrity, and availability, in all its forms, are of crucial importance for the continued operation and governance of the Group. Lack of adequate information security increases the risk of financial and reputational impact from which it may be difficult to recover.

This Policy constitutes the commitment of the Management to the orientation of the Group in terms of information security. Provides necessary information security Management direction and in accordance with business requirements and relevant laws and regulations.

The policy was based on international information security, the best practices and standards (ISO/IEC 27001: 2022). The purpose of this policy is to support an Information Security Management System (ISMS), which will ensure the Group's information confidentiality, integrity and availability.

Our strategy:

- The implementation of the information security system aims to:
- Ensure the protection of all Group information systems and mitigate the risks associated with theft, loss, misuse, damage or abuse of these systems.
- Ensure that users are aware of and comply with Policies and Procedures.
- A secure, information systems environment is provided.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure information security training for all employees.
- The Group is protected from any type of damage through the abuse of its IT facilities.
- Ensure a cycle of continuous improvement.
- Ensure the monitoring and investigation of any actual or suspected security incidents and data breaches.

We are committed to:

- Ensure the implementation of the information security policy and its requirements.
- Approves, assesses and updates the Information Security Policy.
- Provide direction and support the people who contribute to the effectiveness of the information security system.
- Support the various roles to demonstrate their information security leadership.
- Ensure mandatory information security awareness training for all employees

THE MANAGING DIRECTOR