Brisa Group Information Security Policy and Standards

Brisa Auto-Estradas

ÍNDICE

1. INTRODICTION

Information is understood to be a set of data obtained in a precise and temporally framed manner which, after being organized for a specific purpose and presented in a context that gives it meaning and relevance, contributes to increasing understanding or reducing uncertainty about a particular topic or subject.

Information can exist in various formats: printed or written on paper, stored physically or electronically, transmitted by post or by electronic means, made available on video and/or audio support or transmitted verbally.

In the development of the Brisa Group's business, information is an essential asset since it leads to an increase in knowledge and a reduction in uncertainty, affecting behavior, decision-making and, consequently, final results. It is therefore necessary to create mechanisms to safeguard and protect it, taking into account its value.

The purpose of this document is to define the group's information security policy and standards, to be complied with by all employees of the bodies/companies, as well as by the external entities under their responsibility.

2. INOFRMATION SECURITY POLICY

The information security policy contains the rules aimed at guaranteeing the preservation of all information relating to Brisa Group companies, in their custody or that has been transmitted to them in any way or is recorded by them, aimed at and/or underlying it:

- Bind bodies/companies and their employees to the need to ensure the confidentiality, integrity and availability of information;
- Safeguarding the protection of personal data of employees, customers, suppliers and partners and any other persons or entities;
- Establish information control and protection mechanisms to prevent and mitigate the risk of unauthorized or improper destruction, misuse, theft, access, copying, alteration or disclosure;
- Ensure that external entities providing services or any type of collaboration with the group's bodies/companies comply with the requirements set out in this document;
- Ensure access to information and its use in accordance with the regulations and legislation in force, as well as the group's policies.

3. FINAL PROVISIONS

All situations not provided for in this document or which give rise to doubts, should be referred to the Compliance and Audit Department (BAE/DCA), which is responsible for finding the most appropriate solution and/or clarification.

BAE's Executive Committee (EC) is responsible for approving this policy, which will be subject to periodic review, whenever necessary, in order to maintain maximum rigor and excellence with regard to the principles and guidelines adopted.