Service Order
no. BAE 002/22

From:		Classification:	Internal (I)
BAE		Issued Date:	17.01.2022
Executive Committee		Start Date:	17.01.2022
To:		Expires:	
Brisa Group		Revokes:	SO no. BAE 004/20
Subject:	Operating Standards		
Sub-Subject:	Brisa Group Policy and Standards of Information Security		

SUMMARY

Updates the policy and standards underlying the security of Brisa Group's information, including its classification, processing and the responsibilities of the various parties involved in its handling.

TABLE OF CONTENTS

1. INTRODUCTION

Information is understood as a set of data obtained in a precise and temporally framed manner that, after being organised with a certain objective and presented within a context that gives it meaning and relevance, contributes to the increase of understanding or the reduction of uncertainty regarding a certain theme or subject.

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

In the development of Brisa Group's business, information is an essential asset since it leads to increased knowledge and reduced uncertainty, affecting behaviours, decision-making and, consequently, final results. It is, therefore, necessary to create mechanisms for its safeguarding and protection, 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 its responsibility.

2. INFORMATION SECURITY POLICY

The information security policy contains the rules aimed at guaranteeing the preservation of all information relating to the companies of the Brisa Group, in their custody or which has been, by any means, transmitted to or recorded by them, with the aim and/or underlying purpose of:

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

It is the responsibility of all group employees, as well as of third parties, to safeguard the interests of the organisation, contributing proactively to the protection of information, through compliance with this policy, internal regulations and legislation in force. In the event of non-compliance, they may be held disciplinary or judicially responsible.

3. BASIC CONCEPTS OF INFORMATION SECURITY AND THEIR APPLICABILITY

Information security is based on the following basic concepts:

- Confidentiality: guarantees that access to certain information is restricted to those who are duly accredited and authorised to do so;
- Integrity: guarantees that the information processed is reliable, maintaining all the original characteristics established by the information owner;
- Availability: guarantees that the information is always available for legitimate use, that is, by all those who are authorised to use it, whenever necessary.

For information management to be effective, it is essential that the level of sensitivity of the information is specified by the bodies/companies, based on criteria of confidentiality, integrity and availability.

3.1. Confidentiality

The confidentiality of a given set of information is determined by the bodies/companies according to the following levels and criteria:

- Public Information: Information that can be freely shared with anyone inside or outside Brisa Group, as this sharing does not compromise the objectives and/or the image of Brisa Group;
- Internal Information: Information relevant to the development of the group's activity whose disclosure to the outside is subject to prior validation, so that access by external entities does not compromise the objectives, the protection of the group’s know-how and/or image. This information should only be shared with the group's employees or with specific business bodies/units.

Information	Descrição
Public (P)	Information that can be freely shared with anyone inside or outside, as this sharing does not compromise the objectives and/or the image of the group.
Internal (I)	Information relevant to the development of the group's activity whose disclosure to the outside is subject to prior validation, so that access by external entities does not compromise the objectives, the protection of the group's know-how and/or image. This information should only be shared with the group's employees or with specific business bodies/units. The availability of this type of information to persons external to the group, even under some type of service provision or collaboration, requires prior authorisation by the body/company responsible for the information and the terms of its use must be ensured by the entity that receives it, in particular that it does not make unauthorised public use of it.
Internal with Personal Data (IP)	Internal information that contains personal data relevant to the development of the group's activity, maintaining what was referred to in the previous point, under "Internal (I)" information.
Confidential (X)	Information that is decisive for the success of the group's business or that is classified legally or contractually as such. This information is restricted to a specific set of people (employees and/or partners), explicitly indicated by name, and their access must be duly authorised by the respective person in charge of the body/company, based on what is strictly necessary for the performance of a given function or activity or what is established in the law on the respective protection, because its disclosure may cause damage with a very high impact on the business, on the image, compromise the group's mission and strategy and/or violate legal or contractual obligations. Access by external entities to personal data is subject to the prior authorisation of the person in charge of the body/company, which can be confirmed whenever necessary, limited to what is strictly necessary for the exercise of the contracted activity or as established by law.
Reserved (S)	Information with a security classification restricted to the group's Management Team.

The classification of information can be dynamic, and information classified at a certain time as confidential may be public at another time. In addition, it should be noted that the classification of information does not affect the duties to which the various entities of the group are subject under the legislation that regulates the respective information, namely that of the processing of personal data.

3.2. Integrity

The integrity of all stored information must be guaranteed in order to ensure that all information is preserved in an authentic manner, i.e. in its original, accurate and complete format, without any alterations, in order for it to serve the purposes for which it was designated.

Guaranteeing the integrity of information is based on the clear definition, within the organisation, of the employees responsible for its handling, materialised through the definition of access controls to it, being essential the definition of guidelines and identification of the respective risks for the subsequent implementation of controls and security mechanisms(firewall, definition and revision of access profiles, cryptography, and backups, among others) according to their criticality for the bodies/companies.

3.3. Availability

The information should be classified by the bodies/companies, according to the risk that the loss of its characteristics and/or its unavailability bring to the company's activity, considering the following levels for this purpose:

Informação	Descrição
Very critical	When the unauthorised processing of information, loss or destruction through malicious activity, accident or irresponsible management, causes losses that are difficult to recover or even irrecoverable, with very significant financial costs, placing the body/company in a situation of legal and/or contractual non-compliance and with adverse reputational impact on interested parties.
Critical	When the unauthorised processing of information, loss or destruction through malicious activity, accident or irresponsible management, causes losses or damage which, even if recoverable, has significant financial costs, placing the body/company in a situation of legal and/or contractual non-compliance and with adverse reputational impact on interested parties.
Non-critical	When the unauthorised processing of information, loss or destruction, causes little more than a temporary inconvenience, with limited recovery costs and without any adverse impact on the interested parties.

In order to protect Very Critical or Critical Information, its integrity and compliance with the access regime should be periodically checked, as well as, if applicable, ensuring that there is a second repository, in a different location, that allows the recovery of information in the event of a disaster/catastrophe.

Measures to protect information considered Non-Critical, include the storage of copies in closed places and access control mechanisms, which prevent unauthorized persons from accessing and processing existing information.

4. SAFEGUARDING, PROCESSING AND PROTECTION OF INFORMATION

4.1. Formalisation of Confidentiality Obligations and About the Processing of Information

In the scope of contracting services to external entities, their access to information should always be evaluated and, if necessary or convenient, alternatives should be analysed.

If it is found that access is really necessary, the bodies/companies responsible for monitoring these entities, must take the necessary steps to ensure the commitment of confidentiality and treatment of information between the parties, with a view to safeguarding the interests of the group and the compliance with legal or contractual confidentiality obligations.

When formalising a contractual relationship with a third party, in addition to complying with the legislation and rules in force and the applicable internal policies - namely Brisa Group's Purchasing Management Policy - the existence of confidentiality and information processing agreements (obligations), in close collaboration with the Legal Department (DJR) of Brisa Auto-Estradas (BAE), must be guaranteed, whenever the external entity:

- Accesses information from bodies/companies and/or shares information about its activity;
- Accesses and/or shares information associated with commercial proposals or any other information that is legally or contractually subject to confidentiality obligations;
- Accesses and/or shares personal data (employees and customers, among others).

Additionally, employees should, when accessing information from an external entity, act in accordance with the terms of the confidentiality agreement and/or specific clause in force between the parties.

In the event that there is no confidentiality and information processing agreement or any specific rule on the matter, employees must, with regard to the confidential information of an external entity entrusted to their care, process it in accordance with the provisions hereof in relation to confidential information of the group, without prejudice to the principles and rules applicable through other policies and procedures of the group.

Employees must immediately inform their superior as soon as they become aware of the unauthorised disclosure or possession of confidential information by a third party, as well as take reasonable measures to minimise or correct the dissemination and/or disclosure of the information in question.

In the case of specific projects in which the employees involved need access to confidential information of a particularly sensitive nature, either internal or belonging to third parties, the employees involved may be asked to sign a document demonstrating that they are aware of the characteristics of the information in question and of the level of confidentiality required. This document aims to reinforce the obligations contained in this policy and make clear the confidentiality and sensitivity of the information in question.

4.2. Processing of Confidential Information

Employees and contracted external entities that have access to confidential information must be clearly identified, either by name or by the functions they perform or, in the case of external entities, by the name of the company and/or that of the individual and the activities they perform.

Personal data of employees, customers, suppliers or partners of the bodies/companies are considered to be confidential information.

Access to confidential information can only be granted after permission from the respective heads of the bodies/companies, and this authorisation must be documented physically or electronically.

For information classified as confidential, it must be guaranteed by the heads of the bodies/companies that:

- Tangible records (paper documents, microfilm, among others) are:
  - Stored in places with restricted access, when not in use, with access to these places limited to authorised persons;
  - Physically destroyed when they are no longer needed or, in the case of personal data, when the defined conservation period has expired;
- Any information that is transmitted must, whenever possible, be encrypted, except in cases where this is prohibited by law;
- Portable equipment and/or other mobile and/or external storage devices that have this type of information stored, have encryption technology;
- Servers that store confidential information must be protected by perimeter security barriers, allowing only connections to authorised systems, using only approved protocols for this purpose.

5. FINAL PROVISIONS

This policy applies to all BAE bodies and companies in a relationship with Brisa Group, as they are wholly owned by BAE, as well as to its employees, and its adoption is recommended for companies in which BAE has a shareholding.

All situations not mentioned in this Service Order, or which raise doubts, should be forwarded to BAE's Audit, Organisation and Quality Department (DAQ), which is responsible for finding the most appropriate solution and/or providing clarification.

It is the responsibility of BAE's Executive Committee (EC) to approve this policy, which will be subject to a periodic review, whenever necessary, in order to maintain maximum rigour and excellence regarding the principles and guidelines adopted.

São Domingos de Rana, 17 January 2022

António Pires de Lima, *Chairman*