



INFORMATION SECURITY MANAGEMENT SYSTEM

ISMS POLICY

Document No: BS.PT.079

Issue Date: 01.05.2020

Revision No. / Date: 01 – 15.06.2026

Page Count: 1

REVISION HISTORY

Revision No.	Reason for Revision	Date
00	The document was prepared and incorporated into the management system.	01.05.2020
01	Cover page and revision history were added.	15.06.2026



ISMS POLICY

Document Code:	Initial Issue Date:	Revision No. – Date:	Page No.:
BS.PT.079	01.05.2020	01 – 15.06.2025	1 / 1

In accordance with the main theme of the ISO/IEC 27001:2022 Information Security Management System (ISMS), namely “Information Security Activities,” the organization is committed to ensuring the effective management of information security across its people, infrastructure, software, hardware, organizational information, third-party information, and financial resources; ensuring effective risk management; measuring the performance of information security management processes; and establishing and maintaining appropriate arrangements for information security-related relationships with third parties.

Accordingly, the objectives of our ISMS Policy are to:

- *Manage information assets; identify their security values, requirements, and associated risks; and develop and implement appropriate controls to address identified security risks.*
- *Define the framework and methodology for identifying information assets, their values and security requirements, vulnerabilities, threats to assets, and the likelihood or frequency of such threats.*
- *Establish a framework for assessing the impact of threats on the confidentiality, integrity, and availability of information assets.*
- *Establish the principles and procedures for the treatment of identified information security risks.*
- *Continuously monitor information security risks by reviewing technological requirements and expectations within the context of the services provided.*
- *Fulfil applicable national and international regulations, legal and regulatory requirements, contractual obligations, and information security requirements arising from corporate responsibilities toward internal and external stakeholders.*
- *Reduce the impact of information security threats on business and service continuity and contribute to the continuity of critical services and operations.*
- *Maintain the capability and competence to respond promptly to information security incidents and minimize their potential impact.*
- *Maintain and continually improve the organization's information security level through a cost-effective and risk-based control framework.*
- *Protect and enhance the organization's reputation against adverse impacts arising from information security risks and incidents.*
- *Ensure the continuity and effectiveness of the Information Security Management System.*
- *Continually improve the Information Security Management System and its effectiveness.*

The organization is committed to ensuring that this policy is communicated, understood, implemented, and maintained at all relevant levels of the organization and is reviewed periodically to ensure its continuing suitability, adequacy, and effectiveness.

<u>PREPARED BY</u>	<u>APPROVED BY</u>
Information Security Management System Team	General Manager