Information Security Policy

I. OBJECTIVE

To define a referential framework that contains the organization's essential guidelines with respect to information security, in order to ensure the integrity, confidentiality, and availability of the Company's information, including but not limited to the management, custody and use of the assets considered in the policy.

II. SCOPE

The scope of this policy includes all of SMU S.A. and its subsidiaries ("SMU" or the "Company") and is applicable to all information assets belonging to the organization currently or in the future, and compliance with the policy is mandatory for all Company employees and external contractors. The policy applies to all forms of information and means of transmission, including hard copies, written, digitally or physically stored, shown in presentations, or transmitted verbally.

III. POLICY

SMU considers information to be a valuable asset that must be duly protected, and the Company therefore commits to establish mechanisms that guarantee the effective use of information throughout its life cycle. SMU deems the following objectives and guidelines to be essential for safeguarding information, in compliance with regulations in force:

1. To uphold the principles of confidentiality, integrity, and availability in accordance with the Company's strategic goals.
2. To guarantee that security is an integral part of the life cycle of information systems, applying controls that are appropriate based on the classification of the information in order to minimize IT risks.
3. To guarantee operating continuity in the face of contingencies, protecting the internal and external processing facilities and technological infrastructure that support critical processes.
4. To guarantee compliance with legal, regulatory, and contractual obligations relating to information security.
5. To strengthen the information security culture within the Company, so that all members of the organization understand that they are all responsible for information security.

The specific obligations relating to information security, such as Access Control, Operations, Communications, and Compliance, are described in the Information Security Standards document.

This policy must be kept updated by the Information Security Officer, and any changes must be approved by the Information Security Committee. The policy must be reviewed at least once a year and updated each time changes are made to the mission, strategic objectives, services, infrastructure, and/or procedures related to the safeguarding of information.

In order to ensure the proper use of information assets, the Company reserves the right to audit—at any time and without advance notice—compliance with guidelines related to the access to and use of information assets by users.

Compliance with this policy and any related regulations or procedures is mandatory for all of the Company's employees, and failure to comply constitutes an offense that will be sanctioned accordingly.