PHISHX

INTRODUCTION TO SECURITY POLICY

Objective

The objective of the security policy is to promote best practices, standards and guidelines for our environment in the treatment of information assets, disseminating a culture of information security, maintaining the security of systems, the integrity and availability of data, the confidentiality of information , business continuity and adherence to the laws and regulations that regulate our business.

This policy and the other procedures that support its implementation follow our other policies.

Assets

All technological resources available, such as servers, computers, e-mail, telephones, networks, Internet access and systems are intended solely and exclusively for the interests of the business, in which all employees are responsible for the correct handling and must ensure and protect with purpose of generating benefits to the organization and, as a consequence, assisting in the fulfillment of its mission.

Information

Information accessed, generated, or developed on the institution's internal or external premises by employees or business partners are considered intangible assets and must be properly handled, protected, and used only for the purpose previously authorized, regardless of how it was stored or shared.

Use of Software

Employees must use only the software installed by the information technology team, which is duly registered, approved and licensed by the institution, with a software standard that must be obeyed by all employees. The use or installation of programs that have not been bought, approved, and licensed by the company is not allowed.

INTRODUCTION TO SECURITY POLICY

Use of E-mail

E-mail is limited to business only, and no message may have abusive, obscene, or insulting comments or any other material that could bring bad publicity or public embarrassment to the company, our customers or service providers.
Avoid using e-mail to exchange confidential or strategic messages for the institution's business.

Information Classification

Classifying information is the most important procedure that allows the differentiation of an institution's information through a set of criteria, namely: degree of confidentiality, availability, and integrity.

Life cycle

All information has a life cycle that is divided into: Handling, Storage, Transport and Disposal.

• Handling: the owner handles labeling and classifying it according to the classification of the information.

• Storage: each custodian will handle guarding the information through technology devices and / or partners, ensuring its availability, confidentiality, and integrity.

• Transport: any means, whether physical or logical, must reflect the controls proportional to the classification of the Information and the inherent risks, and always occur in a safe manner.

• Disposal: final process in the information life cycle. Efficient non-recoverable deletion mechanisms, such as paper shredders or digital data cleaning processes, should be used.

Principles of Information Security

We need everyone to respect the following security principles:

• Confidentiality: guarantees that the information processed is the exclusive knowledge of persons authorized to access it.

• Integrity: ensures that the information is kept intact, without undue modifications, whether accidental or purposeful.

• Availability: ensures that the information is available to all persons authorized to consult and / or treat it.