INFORMATION SECURITY POLICY
GRUPO EMPRESARIAL COLOMBINA

OBJECTIVE

Establish the general information security policy for the companies within Grupo Empresarial Colombina, in order to comply with the requirements defined in the security management system, which will support the implementation of controls to preserve the confidentiality, integrity, and availability of information in the companies.

SCOPE

This policy must be complied with by executives, employees, and suppliers who have officials performing activities for the company.

GENERAL CONDITIONS

Information Security Objectives

Colombina, aware of the need to meet the demands of its stakeholders and legal and regulatory requirements, establishes a management framework to initiate, control the implementation, and operate information security within the organization. Based on the above and considering the Information Security Policy of Colombina, the following information security objectives have been defined:

a. Ensure the proper functioning of all information systems in the organization, supported by the implementation of an information security strategy.

b. Ensure that information security risks within the scope of Colombina's Information Security Management System (ISMS) are identified, assessed, and treated based on risk acceptance criteria permitted by management.

c. Comply with legal, regulatory, and contractual requirements supported by the information security strategy.

d. Foster a culture and awareness of the importance of information security in the activities carried out by all employees of the organization.

Information Security Policy Statement

Colombina applies information security strategies considering the organizational context and risk management, aiming to ensure compliance with legal, regulatory, contractual, normative, and technological requirements of its stakeholders.

Furthermore, the organization recognizes that information is a vital asset, and thus establishes and maintains information security management to promptly identify and address risks that may affect the confidentiality, integrity, and availability of information, personal data, and their containers. It also aims to protect them from potential malicious attacks or cyber threats, providing security and trust to meet the needs of stakeholders in service provision.

Taking into account the information security objectives outlined in this document, the companies within the Colombina Business Group, under the ISMS, will undertake activities to ensure compliance, monitoring, and updating of these objectives.

Information Security Governance

Executive Management Commitment: It allocates the necessary resources (human, technological, and financial) and promotes awareness, training, and consciousness to foster a culture of security for continuous improvement.

Information Security Committee: This committee holds decision-making power within the organization as the highest authority regarding information security within the management system.

Information Technology Department: It is responsible for supporting proposals and implementing technical measures concerning information security, aligning the guidelines defined in the policies with technological components.

Fundamental Principles

Colombina has established the following fundamental principles that support the Information Security Policy:

a. Information is one of the most important assets of Colombina, and, therefore, must be used in accordance with the organization's requirements while preserving security criteria (Confidentiality, Integrity, and Availability).

b. The confidentiality of information within the organization, as well as that belonging to third parties, must be maintained regardless of the medium or format in which it is found.

c. The information of the organization must be preserved in its integrity, regardless of its temporary or permanent residence, or the way it is transmitted.

d. The organization's information must be available when required and by authorized users. It should also be presented in a timely manner when required by legal and regulatory requirements.

DEFINITIONS

Information Asset: Anything that has value for the organization and, therefore, must be protected, such as physical and digital information, software, hardware, services, and/or people.

Confidentiality: A characteristic that indicates that the information asset is only accessed by authorized personnel, processes, systems, or entities.

Availability: A characteristic that indicates that the information asset is timely and can be accessed and used by authorized individuals, entities, or processes when required.

Integrity: A characteristic that ensures the accuracy, quality, truthfulness, and completeness of the information asset.

Mobile Devices: Small-sized devices that generally have special processing capabilities, a permanent or intermittent connection to a network, limited memory, and are associated with the individual use of a person who can configure it according to their preferences.

Partners: Companies with which an alliance contract has been signed.

Information Security Management System: A set of processes and procedures aimed at the planning, construction, monitoring, and continuous improvement of an organization's information security.