INFORMATION SECURITY POLICY

OBJECTIVE

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

SCOPE

This policy must be adhered to by managers, employees, and suppliers who perform activities within the Information Technology area.

CONDITIONS

The purpose of this document is to inform the employees of the Colombina Business Group about the Information Security Policy established for the protection of the organization's information.

This document includes the aspects that all employees must consider to ensure that information is accessed only by those who have a legitimate need to perform their functions within the organization (Confidentiality); that it is protected against unauthorized modifications, whether intentional or unintentional (Integrity); that it is available when required (Availability); that it is used for the purposes for which it was obtained (Privacy); and that a record of the events that occur when accessing the information is maintained (Auditability).

Therefore, employees of the Colombina Business Group must act in accordance with the guidelines set forth in this document and those developed in each specific Security Policy, as well as the standards and procedures that are part of information security. This is understood with the commitment of senior management to support all necessary activities to achieve the goals and principles of information security, in line with the responsibilities assigned within the defined Roles and Responsibilities related to this matter.

This document describes the objective, scope, fundamental principles, roles, and responsibilities. Additionally, this policy generally references the individual security policies, which specify the stance adopted by the Colombina Business Group in managing its information and the actions that must be taken to achieve the objectives of this Policy. These individual policies are further detailed in the "Manual of Computer Security Policies."

STEPS TO FOLLOW

DECLARATION OF THE INFORMATION SECURITY POLICY

The Colombina Business Group applies information security strategies that consider the organizational context and risk management to ensure compliance with legal, regulatory, contractual, normative, and technological requirements of its stakeholders.

Furthermore, it is acknowledged that information is a vital asset for the organization, which is why the Group establishes and maintains information security management aimed at identifying and promptly addressing risks that may affect the confidentiality, integrity, and availability of information, personal data, and their containers, as well as protecting them from potential malicious attacks or cyberattacks, providing security and trust to meet the needs of stakeholders in the provision of services.

Considering the information security objectives established in this document, the companies of the Colombina Business Group, within the Information Security Management System (ISMS), will develop activities that allow for compliance, monitoring, and updating of these objectives.

Senior Management Commitment

As part of its commitment, senior management allocates the necessary resources (human, technological, and financial) and promotes awareness, training, and consciousness-raising to foster a culture of security for continuous improvement.

Finally, to comply with this policy, support is provided through the "Manual of Computer Security Policies," the personal data protection policy, and a set of procedural and technological controls.

Updates to the Information Security Policy

The Information Technology department conducts an annual review of the information security policies, and their updates will depend on internal and external factors. Internal factors may include the needs of the companies regarding information security and structural changes. External factors may include changes or updates to the ISO/IEC 27001:2013 standard and/or Colombian legislation on matters related to data privacy or information security, market regulation, technology, or other applicable factors.

Exceptions

Exceptions to these policies must be approved by the person responsible for Information Security, the Head or Leader of Information Technology for each of the companies within the Colombina Business Group, or the person they designate.

ACCEPTANCE OF THE POLICY

It should be considered that, by using any information asset of the companies within the Colombina Business Group, it is mandatory to respect and accept the terms and conditions of this policy. In some cases, due to legal requirements, you may be asked to sign a confidentiality agreement in which you commit to following the rules and conditions for using any information asset. At all times, you must comply with all licensing requirements and confidentiality agreements requested by the companies.

FUNDAMENTAL PRINCIPLES

The Colombina Business Group has established the following fundamental principles to support the Information Security Policy:

a. Information is one of the most important assets of the Colombina Business Group and therefore must be used according to the organization's requirements while maintaining security criteria (Confidentiality, Integrity, and Availability).
b. The confidentiality of the organization's information, as well as that belonging to third parties, must be maintained regardless of the medium or format in which it is found.
c. The organization's information must be preserved in its integrity, regardless of its temporary or permanent location or the way it is transmitted.
d. The organization's information must be available when required and to those who are authorized to use it; likewise, it should be presented promptly when required by legal and regulatory requirements.
e. The organization's information that is stored, collected, and/or processed through technologies utilizing artificial intelligence (AI) components, data mining, and other emerging technologies must be protected against potential risks and vulnerabilities to which they may be exposed, thus ensuring the accuracy, truthfulness, and completeness of the data.

INFORMATION SECURITY OBJECTIVES

The Colombina Business Group, aware of the need to meet the requirements of its stakeholders and the legal and regulatory requirements, establishes a management framework to initiate and control the implementation and operation of information security within the organization. Based on the above and considering the information security policy of the Colombina Business Group, the following information security objectives have been defined:

a. Ensure the proper functioning of all the organization's information systems and the use of emerging technologies (artificial intelligence, data mining, data analytics, etc.) in the development of processes, supported by the implementation of an information security and cybersecurity strategy.

b. Ensure that the information security risks within the scope of Colombina's ISMS are identified, assessed, and treated according to the risk acceptance criteria allowed by Management.
c. Comply with legal, regulatory, and contractual requirements, supported by the information security strategy.
d. Create a culture and awareness of the importance of information security in the tasks performed by all the organization's employees.

ROLES AND RESPONSIBILITIES

All roles and responsibilities for information security are defined in the "Information Security Roles and Responsibilities Manual." Information security should be integrated into the organization through policies or the creation of procedures, standards, formats, and guidelines.

INDIVIDUAL SECURITY POLICIES

The individual policies for information security are defined in the "Information Security Policy Manual," which is available for consultation in the internal repository.

DOCUMENTARY REFERENCES

ISO/IEC 27001

ANNEXES

Information Security Policy Manual

Information Security Roles and Responsibilities Manual

DEFINITIONS

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

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

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

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

Artificial Intelligence (AI): A field of computer science that includes machine learning and deep learning, which involves developing AI algorithms modeled after human brain decision-making processes. These algorithms can "learn" from available data and make increasingly accurate classifications or predictions over time, allowing computers to simulate human intelligence and problem-solving capabilities.

Mobile Devices: Small-sized devices that typically have special processing capabilities, continuous or intermittent network connectivity, limited memory, and are usually owned and operated by individuals who can configure them to their liking.

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

Information Security Management System (ISMS): A set of processes and procedures aimed at planning, building, monitoring, and continuously improving an organization’s information security.