CORPORATE CYBERSECURITY POLICY

Version	Description of changes	Approval	Effective
1.0	Initial version	Cybersecurity Committee	December 2018
2.0	Update of concepts and participants of the cybersecurity committee.	Cybersecurity Committee	July 2021
3.0	Update of applicable regulatory frameworks and general principles	Cybersecurity Committee	June 2025

INDEX

1. Objective....3
2. Scope....3
3. Cybersecurity Policy....3
3.1 Regulatory Structure....5
3.2 General principles....5
3.4 Structure, Roles and Responsibilities....6
4. Transition period....7
5. Track changes....7

1. Objective

This corporate policy provides a framework of action and commitment, which enables the definition of effective security management processes for Andina's Information assets. These assets are understood as all those elements relevant to the production, emission, storage, communication, visualization and recovery of information valuable to Andina, regardless of its format, medium or support in which they reside. This also includes the equipment, networks and systems that support this information and facilitate the development of Andina's commercial and/or business activities. These systems encompass all versions in production, development, test, pre-production or any other phase involved in the provision of services. This referential framework aims to establish a control model that safeguards the confidentiality, integrity and availability of the Information assets. Furthermore, it ensures compliance with applicable laws and regulations in force, in accordance with the legal frameworks of the countries where Andina operates, while maintaining a balance between risk levels and the efficient use of resources.

2. Scope

This policy, along with the documents derived from it, applies to all personnel of Coca-Cola Andina, its subsidiaries, and third parties providing services related to the regulated matters, as well as to stakeholders who access Coca-Cola Andina’s information. Unless otherwise specified, this policy must be adopted and integrated into the daily activities of all personnel of Coca-Cola Andina and its subsidiaries. Additionally, the Manual for the Use of Digital Information Assets sets forth the guidelines applicable to all personnel.

3. Cybersecurity Policy

This Policy serves as the primary document of the cybersecurity regulatory framework, from which norms, standards, procedures, and/or manuals are derived. These cover areas of Cybersecurity associated, among others, with:

- Human Resources: A rule that establishes the need to educate and inform personnel—both upon entry and on an ongoing basis, regardless of their employment status—about the information security measures relevant to their roles and the cybersecurity expectations placed upon them.
- Logical Security: A standard that defines the guidelines to ensure the secure use of information systems, aiming to protect the confidentiality, integrity, and availability of Coca-Cola Andina's critical information resources.
- Secure digital development: A standard that outlines general information security guidelines for the development, acquisition, or maintenance of Coca-Cola Andina’s information systems, in accordance with the software development life cycle and the applied methodological framework.

- Physical Security: A standard that sets forth guidelines for implementing controls to prevent physical threats to company facilities and critical resources, including unauthorized access and physical damage to information processing equipment or system interruptions.
- Use of digital information assets, applications and technological devices: A manual that defines specific security guidelines for the safeguarding and acceptable use that each of the collaborators is responsible for applying on digital information assets, applications and technological devices provided by the company, such as collaboration tools, email, video conferencing, instant messaging, and digital devices, computers, notebook, cell phones, mobile equipment, and their access to the internet for the digital exchange of information. The objective is to protect them from multiple internal or external threats, ensuring the integrity, confidentiality and availability of the resources that the company makes available to the collaborators for the fulfillment of their tasks and for use primarily for business purposes of the company and development of the functions entrusted. The goal is to protect against internal and external threats, ensuring the confidentiality, integrity, and availability of resources used primarily for business purposes and the performance of assigned duties.
- IT Risk Management: A methodology that provides the necessary guidelines to effectively evaluate, measure and manage risks associated with technology.
- Cybersecurity Monitoring: A standard that governs the execution of risk analyses and periodic or on-demand audits. Its purpose is to verify compliance with information security policies, detect potential security breaches requiring corrective actions, and monitor user or system activities as needed.
- Cyber Resilience Form Coca-Cola Andina suppliers: A form used to measure indicators of maturity levels in order to assess the resilience of third-party service providers in the IT (Information Technology) and OT (Operational Technology) domains, with respect to the objectives of Anticipate, Resist, Recover, and Evolve.
- Information Security: A policy designed to establish general guidelines regarding the responsibility, safekeeping and risk management of information. It also provides general guidelines on access, manipulation, processing, transmission, protection, storage or any other activity carried out on Coca-Cola Andina's information assets.
- Cyber-attack response and recovery plan: A plan that ensures the implementation of a rapid and effective procedure to act in the event of information security incidents, particularly those associated with cybersecurity attacks. This plan also includes measures to contain damage, ensure appropriate communication of the incident to the responsible parties—both inside and outside the company—and establish mechanisms to document incidents with supporting evidence, with the goal of preventing recurrence.

3.1 Regulatory Structure

The Cybersecurity Policy and the documents emanating from it constitute the fundamental framework within which digital activities for the protection of information assets must be integrated. These guidelines establish a basic set of rules, from which detailed standards, procedures, and/or manuals must be formulated to meet the requirements set forth in the standards of the areas outlined in point 3.

3.2 General principles

As a general guideline, Coca-Cola Andina's cybersecurity:

Adds value to the company. Cybersecurity is justified as it adds value to the process chain and, ultimately, to the company as a whole.

It is transversal to the company. The responsibility for the application of cybersecurity controls at Coca-Cola Andina is not limited exclusively to the Technology management. Its principles must also be applied across commercial, business, human resources, financial, and other processes, policies and procedures at both the operational and corporate level. This comprehensive vision is what ultimately contributes to achieving the company's cybersecurity objectives.

We all build it in a permanent effort. Cybersecurity is achieved because all collaborators, in every activity they perform, think and act with digital information security conditions in mind.

It must be in accordance with the requirements of the environment. All efforts to implement cybersecurity must comply with applicable laws, regulations, requirements and standards of the industry and the market in which we operate.

It requires a person in charge and allocation of resources. Considering the degree of importance that Coca-Cola Andina is assigning to cybersecurity, the necessary human and financial resources will be allocated in order to achieve the defined level of cybersecurity, including the allocation of a specific item in the annual budget for this objective.

Continuous improvement. Commitment to the ongoing review and updating of security measures to adapt to emerging threats and evolving technologies. This includes, among other actions, the review of policies, manuals, procedures, security controls and personnel training.

Identify, Protect, Detect, Respond and Recover. Strengthen the development of cybersecurity capabilities across 5 key pillars, within a continuous monitoring model to enable a proactive response to digital threats and ensure the protection of information assets, cyber assets and critical technology infrastructure managed in Coca-Cola Andina and its subsidiaries in all countries where the company operates.

3.3 Guidelines and key concepts:

Cybersecurity is a concept that encompasses the set of actions aimed at protecting information present in cyberspace, as well as the infrastructure that supports it.

Cyberspace is a virtual environment that includes all information technology systems that depend on the availability of private or public networks enabling digital data interaction.

The working and control framework implemented within the organization is based on a subset of recommendations and practices derived from recognized standards, such as CIS (CSC 7.1), COBIT 5, ISO (ISO 27001 / 27002:2013), and NIST (NIST SP 800-53 Rev. 4 / NIST 800-82 rev2 and NIST CSF v1.1).

Information, processes and support systems are considered critical business assets and must be safeguarded at all times by all collaborators and suppliers.

Achieving and maintaining the required levels of cybersecurity involves investments and costs. Coca-Cola Andina is committed to maintaining a balance between market security standards, the guidelines of The Coca-Cola Company, the board of directors' defined risk tolerance the investment and costs involved.

3.4 Structure, Roles and Responsibilities

A committee has been established for the strategic management of cybersecurity, whose role is to review and approve the direction and strategy regarding cybersecurity and contingency issues presented by the Technology Security Management. It is also responsible for defining the level of cybersecurity the company must maintain, as well as the standards and/or procedures to be published. The cybersecurity committee will be coordinated by the Technology Security Management. This cybersecurity committee will convene annually or as necessary, to address contingent issues or make decisions. It is composed of the following members: Chief Human Resources Officer, Chief Legal Officer, Chief IT Officer, Corporate Manager of Management Control, Risk and Sustainability, Corporate Internal Audit Management Representative and the IT Security Manager.

The IT Security Management is responsible for developing, promoting and coordinating the implementation of security and technological contingency actions and initiatives at the corporate level.

The technology teams, represented by managers, technical leaders, architects and specialists, are primarily responsible for ensuring that the policies, norms, standards and associated security procedures are respected within their respective units and work areas.

It is the responsibility of all Coca-Cola Andina personnel to work in compliance with the defined security policies, standards and procedures. This includes executing the established controls and participating in training and awareness programs aimed at minimizing risks in the handling of digital information essential to their roles. Under no circumstance or pretext may any individual covered under the Scope of this policy engage in illicit conduct involving the Company's information assets- whether under direct instruction from a superior or under the pretext that the conduct benefits Coca-Cola Andina. Non-compliance with the cybersecurity policies, standards, procedures and manuals, as well as the improper and/or illegal use of information assets may result in disciplinary action, including termination of employment, and other legal consequences, as outlined in the Internal Regulations of Order, Hygiene and Safety applicable to each operation.

All collaborators are required to report any incident, vulnerability, activity or situation that could affect the security of the company's information assets, using the designated reporting channels.

The role of internal audit is to provide an independent assessment of the control models implemented, ensuring adherence to the guidelines approved, communicated and published as outcomes of the committee's sessions and therefore, its participation in committee meetings is exempt from approving or rejecting matters submitted for consultation.

4. Transition period

This new version of the policy has no transition period and will be applied immediately upon publication.

5. Track changes

Version	Description of main changes (for further background, contact: politicascorporativas@koandina.com)	Approval	Validity
1.0	Initial version	Cybersecurity Committee	December 2018
2.0	Update of concepts and participants of the cybersecurity committee.	Cybersecurity Committee	July 2021
3.0	Update of applicable regulatory frameworks and general principles	Cybersecurity Committee	June 2025