CYBERSECURITY POLICY

ARGOS

Content

1. OBJECTIVE

Establishing frameworks that will guide the behavioral guidelines for employees and third parties involved in the handling of information and operations, as well as the protection measures for the technologies that enable business. Through the policy, guidelines are set for the implementation of action plans that ensure the company's cybersecurity.

2. SCOPE

This policy applies to all geographical locations where Cementos Argos S.A. (hereinafter referred to as "Cementos Argos") operates. Additionally, it is mandatory for all employees and individuals or entities who are involved with the company's information technology and operations to comply with this policy.

3. POLICY

CYBERSECURITY POLICY

Cementos Argos, in compliance with laws and regulations for the protection of physical information assets[1], digital, and cyber assets[2] in the countries where it operates, and in line with its technology policy and personal data treatment policy, identifies, manages, and mitigates associated risks through the implementation of best practices in cybersecurity[3]. The aim is to ensure the confidentiality, integrity, reliability, and availability of information, information technologies, and operational technologies to secure business sustainability and the safety of individuals.

[1] Information asset: a collection of data, including personal data, that is collected and transformed and holds strategic, operational, economic, technical, legal, or regulatory value for the business; therefore, there is a need to protect them.

[2] Cyber asset: a programmable electronic device and elements of communication networks, including hardware, software, data, and information. It also includes elements with routable communication protocols that allow local or remote access to it.

[3] Cybersecurity: refers to the protection of computer systems, networks, and connected devices against digital threats such as data theft, service disruption, or unauthorized access. It involves the use of appropriate technologies, processes, and practices to safeguard against these threats.

Regarding cybersecurity, the company, its employees, and third parties involved with digital assets commit to:

- Ensure that the cybersecurity policy is aligned with the company's objectives and serves as a mechanism to contribute to the organization's continuity and value.
- Actively support cybersecurity within the organization to comply with relevant standards and achieve defined objectives, considering that cybersecurity is a shared responsibility among all members of the organization.
- Adopt a risk management-based approach that allows the company and its employees to freely, securely, and reliably carry out their activities in the digital environment.
- Use all information stored, created, or transmitted using Cementos Argos resources exclusively for the organization's purposes and business objectives.
- Maintain an up-to-date inventory of information assets and existing cyber assets, including their classification and ownership.
- Establish controls to prevent loss, damage, theft, or malfunction of information assets and cyber assets that may lead to business disruptions or harm to the organization through the identification, assessment, and treatment of risks, threats, and vulnerabilities in information and operational systems.
- Ensure the establishment of measures for the proper functioning of the technological infrastructure to guarantee the confidentiality, integrity, and availability of information assets and cyber assets, including measures that ensure the non-repudiation of actions by internal and external actors in the digital environment.
- Engage employees and third parties involved in the digital environment to understand and apply controls to protect information assets and cyber assets, reducing the risk of human errors, theft, fraud, or misuse.
- Access only information related to their job functions and responsibilities. Third parties requiring access to information systems only access the information necessary for the execution of their contractual obligations.
- Disseminate and promote, in a planned manner, the objective of cybersecurity, its characteristics, and individual responsibilities to achieve it, including annual training plans, as well as ongoing activities and induction processes for new staff.
- Effectively manage cybersecurity incidents to minimize the risk of loss of availability, confidentiality, reliability, and integrity of information assets and cyber assets, and to identify the controls to be implemented.

- Ensure that all critical processes and information systems containing information assets have continuity plans that ensure resilience and timely recovery according to business requirements.
- Promote the responsible use of artificial intelligence tools, ensuring their implementation with appropriate security measures to protect the integrity and confidentiality of the data.
- Ensure that the use, operation, and management of information systems comply with the requirements of applicable national and international laws regarding software licensing, copyright, information privacy, information record retention, and all current legal provisions.
- Respect the privacy of customers, employees, suppliers, and other third parties associated with Cementos Argos, and take reasonable measures to guarantee the security of personal data collected, stored, processed, disclosed, and transmitted.
- Collaborate with the technology department in the development, adoption, or procurement of new applications or technological services, ensuring compliance with cybersecurity guidelines and standards, and their proper integration with the company's solutions ecosystem.
- Comply with the cybersecurity policy and its guidelines. Any violations by employees and third parties involved with digital assets will result in incident treatment measures and disciplinary actions by the human resources department.
- Ensure information security and operational continuity by investigating the digital behavior of users, carried out by internal control and cybersecurity departments.

4. GOVERNANCE OF CYBERSECURITY

Cementos Argos and its affiliated companies have defined the following organizational structure with instances, roles, and responsibilities in order to ensure proper compliance with the cybersecurity policy:

Strategic Cybersecurity Committee:

- Approve the organizational strategy that provides direction in cybersecurity management.
- Approve the cybersecurity policy and its guidelines.
- Manage the cybersecurity risk map and evaluate the effectiveness of treatment measures taken.

- Ensure the adoption of recommendations issued by regulatory bodies, auditors, insurance companies, risk areas, among others.
- Report to the board of directors and senior management.

Tactical Cybersecurity Committee:

- Propose guidelines to materialize the cybersecurity policy.
- Identify risks and vulnerabilities in the environment, constantly monitoring the cyber environment.
- Supervise the implementation of security measures.
- Propose the intrusion testing program and simulations for cyber-attacks.
- Adjust the training and awareness program for all members of the organization.
- Design and implement comprehensive communication and training programs to strengthen the culture and capabilities of the cybersecurity management system.
- Communicate and report the organization's cybersecurity status to senior management and other key members of the organization.

Owners of Information and Cyber Assets: Responsible for the assets assigned to them, as well as the classification, control, and monitoring of the use and management of these assets.

Custodians of Information and Cyber Asset: Responsible for safeguarding the assets, enforcing access restrictions and classifications given by the owners.

Control Areas (Technology, Risk, Audit): Responsible for managing and evaluating the measures taken to mitigate the risk associated with cybersecurity.

Chief Information Security Officer (CISO): Responsible for developing the comprehensive cybersecurity management model, framing the cybersecurity policy within this ecosystem, and managing the risks associated with information security and cybersecurity.

Users: Any employee, supplier, contractor, or other authorized third party who uses the companies' information in the execution of their daily work activities.

5. ANNEXES AND REFERENCES

- NIST Cybersecurity Framework CSF, ISO 27000 standards
- Laws and regulations
- Cybersecurity guidelines and annexes
- Technology Policy
- Personal Data Treatment Policy

6. EXCEPTIONS

Not applicable

7. POLICY REVIEW PERIODICITY

Every year or as required.

8. APPROVED BY

Approval instance: Strategic Cybersecurity Committee

Policy owner: Tactical Cybersecurity Committee

VERSION CONTROL

No. Ver.	Chapter	Date	Description
V_001	All	July 17, 2007	Initial Issue
V_002	All	August 09, 2007	Total revision of the document
V_003	All	April 11, 2022	Adjustments opportunities for improvement in Cybersecurity Process Audit
V_004	All	March 28, 2023	Approval Instance Cybersecurity Strategic Committee
V_005	All	February, 2024	Adjustment on Artificial Intelligence in Cybersecurity