Information Security / Cybersecurity Statement

Introduction

At Cencosud, we promote a culture rooted in **passion, respect, transparency, and trust** every day, with the purpose of **serving our customers extraordinarily at every moment** through a **distinctive, sustainable value proposition with high standards of excellence** in products and services. Our Sustainability Strategy and Business Model, based on the principles of Responsible Procurement, Production, and Consumption, guide our Business Units toward becoming a sustainable organization.

In this context, we establish the "Information Security Statement," whose purpose is to define general guidelines that enable the proper management of the confidentiality, integrity, and availability of information, establishing a security and control culture in line with international best practices.

This document is intended for third parties (customers, suppliers, investors, among others) associated with the company and who require knowledge of the security approach adopted by Cencosud.

The statement is subject to annual review and update.

Commitment to Security

As an organization, we reaffirm our commitment to:

- Preserve Confidentiality, Integrity, and Availability of information.
- Comply with laws, regulations, and contracts.
- Shared responsibility at all levels of the organization.
- Risk-based approach.
- Continuous improvement of the Information Security Management System (ISMS).

This commitment explicitly extends to all employees, contractors, suppliers, consultants, investors, and other third parties, who must actively adopt these guidelines as an integral part of their relationship with Cencosud.

Regulatory Framework

The company has a Regulatory Framework based on international standards such as ISO, NIST, and SANS CIS, in addition to complying with applicable local regulations in each country.

Information Security / Cybersecurity Governance

The Group CISO (Chief Information Security Officer) is responsible for leading the implementation of this policy, together with the Information Security Committee and the Information Security teams in each country.

Responsibilities

- All employees must protect the information under their custody.
- Area leaders must ensure compliance with the Regulatory Framework within their teams.
- Suppliers must comply with contractually defined controls.

To ensure effective compliance with this statement, clear responsibilities are defined in the Regulatory Framework and relevant contracts, which must be assumed by all parties involved in Cencosud's operations. Adherence to these is essential to maintain a relationship of trust and continuity with the company.

Information Security Program

Includes:

- Access management.
- Network and system security.
- Physical and environmental security.
- Incident management.
- Business continuity.
- Supplier management.
- Monitoring and auditing.

Security Awareness and Training

Cencosud maintains a continuous awareness program for its employees and third parties to reinforce good practices and mitigate human-related risks.

The program is articulated through defined procedures and specific controls, covering everything from source code review in critical applications to encryption of sensitive data, management of privileged access, and physical security controls at key facilities.

Risk Assessment

Systematic assessment processes are carried out to detect potential threats and vulnerabilities, establishing corrective actions in line with the risk appetite defined by Cencosud.

Incident Management

Incidents must be reported immediately to the Information Security team. The response protocol will be applied according to the level of criticality, including forensic analysis, stakeholder communication, and containment measures. Timely reporting and active collaboration are essential for effective incident management and are part of the commitments assumed in our relationships.

Supplier Security Management

All third parties with access to systems or information must be evaluated and comply with the controls required by the company. Contracts must include security clauses, audit rights, and periodic recertifications.

The process includes formal notification, investigation with forensic support, regional coordination, centralized event logging, and follow-up of corrective actions until documented closure.