Information Security / Cybersecurity Statement

At Cencosud we work daily with **passion, respect, transparency, and trust**, to improve the quality of life of our clients through a **unique, sustainable experience and with unmatched quality standards** in their products and services. Our Sustainability Strategy and Business Model, based on the principles of Supply, Production and Sustainable Consumption, seeks to lead the different Business Units towards transforming the organization into a sustainable business.

Aware of this, the "Information Security Declaration" appears, which aims to provide a summary of the security controls and processes within the Cencosud group. This document is for use with third parties (clients, investors, suppliers, among others) who are related or committed to Cencosud, and who wish to learn about security arrangements within the group. This statement will be reviewed and updated annually.

Regulatory framework

The Company has a Regulatory Framework, based on best practices and international reference frameworks, such as NIST and Sans CIS, which establishes the guidelines and security measures to be considered by the different areas and by all Cencosud Collaborators, in order to ensure the protection of information, in all its forms and means, against its accidental or deliberate modification and unauthorized use and / or disclosure.

Commitment to Safety

Cencosud is committed to continually maintaining and improving security, to meet our responsibilities, with our clients and regulatory bodies, to reduce exposure to risks, legal penalties, operational losses or reputational damage.

As a group, we are committed to:

- The confidentiality of corporate, partner, supplier, and customer information
- The integrity of the information
- The availability of our information
- Compliance with legal, regulatory, and regulatory requirements
- Provide training in information security and risk awareness to all staff
- Report and investigate actual or suspected information security violations.

Organization of Information Risks and Cybersecurity

Cencosud's management as a whole is responsible for identifying, evaluating, and managing the spectrum of risks to which the group is exposed.

Cencosud applies a protection model that guarantees that risks and controls are properly managed within its business, functions, and technology teams, on an ongoing basis.

Information Security / Cybersecurity Governance Structure

- Name: Marcelo Dalceggio
- Position: Chief Information Security Officer

Cencosud Staff

At Cencosud, background checks are a key group-level defense against insider trading and other risks, and minimum background requirements have been defined. All employees of the Cencosud group, including contractors, service providers and contingency workers are subject to a background check, prior to entering a position or performing a function. The background check process also seeks to provide a level of assurance that the background does not raise reasonable concerns that such recruitment could expose the group to unacceptable levels of risk. As a pre-filter for all applicants, a DISC test is performed.

Background checks, as permitted by local law, include when possible:

- Certificate of studies
- Curriculum Vitae
- Job references to former employers (Back Office)
- Course OS10 (Security positions)

Security Awareness

Cencosud has a continuous security awareness program, which uses various channels to download information, in order to involve staff.

This program mainly has:

- On-site and / or virtual training;
- Publication on intranet / posters;
- Awareness campaigns;
- Induction courses for new collaborators.

Cencosud Policy

Cencosud has developed, for the entire group, an Information Security policy, which establishes guidelines for Cencosud, its collaborators and third parties involved.

The policy provides a framework for all security processes and mechanisms. It defines the security objectives, classification, responsibilities, and fundamental principles to ensure it in accordance with the business objectives.

Cencosud's policies include, but are not limited to:

- Defined information security responsibilities for collaborators, contractors and third parties
- Testing to identify missing or poor controls
- Policy and guidelines for all users, about acceptable use of mail and internet
- Defined criteria for access control, including the need to know, privilege principle, unique user / ID, password complexity, access approvals, recertification transfer and abandonment processes (disengagement), privileged access and remote access controls.
- Software development life cycles for applications that include code review, separation of tasks, security reviews for web services, among others.
- Change control and information backup for business continuity.
- Defined processes for information classification
- Detailed instructions for encryption, secure transfer, and destruction of data
- End user environment policies, covering data extraction, non-IT data processing (end user computing), data classification, labeling, secure storage destruction, and remote work.
- Technical configuration and control configuration for IT infrastructure, networks, and platforms.
- Physical security

The policy defines minimum requirements for:

- The management and information management
- Access control
- Physical security
- Communications, operations, and systems development.

Risk Management

Cencosud uses risk management across all of its key lines of defense to identify, report and manage risks across the organization. The information security frameworks within Cencosud follow the best international practice standards.

Risk assessments are performed periodically to address changes in group information security requirements or risk appetite and when significant changes occur. Cencosud performs risk assessments on the variety of strategic / critical assets within the organization. These can be physical assets, people, software, and information. For example, periodic evaluations of the security risk of information on application and infrastructure technologies are carried out to:

- Identify, quantify, and manage information security risks to achieve business objectives.
- Provide means to identify activities and factors that represent the greatest security risk for Cencosud.
- Ensure that information security problems are managed according to their risk rating and that controls are proportional to the level of risk discovered.
- Provide a business vision of information security risks and respective remediation plans to develop the information security strategy.
- Plan the deployment of resources in areas that provide the greatest risk reduction for customer / corporate information.
- Evaluate all aspects of the information security risks, threats and vulnerabilities of our assets.

Access Management

An identity and access management unit owns and operates the access management control within Cencosud, this ensures access management aligned with the regulator and guided by policies throughout the life cycle of support controls.

Identity and access management team services / responsibilities include:

- Controls on new employees, employees who leave the company or move internally, incorporating segregation of duties to ensure that the corresponding level of privilege rights are managed and / or maintained for all user activities.
- Privileged access management controls with due justification and authorization, incorporating activity validation through a registration and monitoring process.
- Access to recertification controls to ensure that accounts and associated rights are reviewed, maintained, or revoked, periodically, by the appropriate reviewer.

Application Security

Technical application security teams identify threats, controls, and perform tests, including:

- Application security consulting and risk assessments: to ensure that risks within Cencosud applications and systems are managed to an acceptable level;
- Technical and information security advice to companies, projects, or function initiatives.
- Definition and testing of application system controls related to information security.
- Contribution to the standards and procedures for building the system.
- Installation and monitoring of application level controls.
- Development of minimum reference security standards.
- Security / application penetration testing (including vulnerabilities covered by the cyber security framework) and code reviews.

Net Security

To allow effective management, Cencosud uses various technologies strategically implemented throughout its network, which are described below:

- Wireless network management
- Denial of Service Protection
- Internet access filter
- Security Infrastructure Testing
- External Audit of Compliance and Information Security

Data Encryption

Cencosud, as a first-rate Company, is aware of the importance of taking care of personal, sensitive, and critical data, treating it in accordance with current privacy regulations in the region.

An example of this is data encryption for all sensitive data for means of payment using EMV technology, for face-to-face transactions and certified payment gateways for non-face-to-face purchases, as well as communications with banks are encrypted and secure.

Host Security

Work Stations (notebook) and mobile devices

Cencosud workstations and laptops have antivirus software built into the default operational builds, configured to automatically check files as part of their regular "full-time" analysis and get updates as they become available.

- Desktop / laptop computers have a pre-installed custom build that limits administrative access for users.
- Access to Cencosud's internal network from outside the office is restricted to authorized devices controlled by industry standard remote connectivity and multi-factor authentication controls.
- Internet access and network connectivity for Cencosud laptops is routed through the Cencosud network. VPN software ensures that Cencosud laptop users cannot connect directly to the public Internet.

Server platform

System security is built into our server platforms.
Hardening measures and controls are built into server builds; these include, but are not limited to:

- Unnecessary and redundant services, devices, processes, protocols, system and network utilities, programs, and accounts are disabled / removed.
- Operations / services are executed with the minimum required privileges; Adequate file system security is applied.
- Strong user account and password controls are implemented for all users who enforce length, complexity, history, and locks. Automated control of passwords with registration and auditing applied to privileged accounts.
- Configuration settings are defined according to the "least privilege" principle.
- Monitoring and reporting of any breach.

Patch management and handling

Frontline teams receive vulnerability notifications from the product vendor and recommended patch responses. The prioritization for implementation in Cencosud's heritage is determined by the patch priority ranking, assigned as part of the assessment process using the Common Vulnerability Scoring System of the industry standard framework.

Patches prior to deployment to production systems are tested in non-production environments worldwide.

All patch deployments are managed following Cencosud's Global Change Management and Incident Management Processes.

Appropriate governance and oversight are exercised through regular engagement and communication with globalcompanies and functions in accordance with the established framework.

Remote Work

The access made by Cencosud personnel to the Company's resources outside the internal network is carried out through the Remote Access mechanism authorized by Computer Security.

Additional controls and guidance for staff working remotely include, but are not limited to:

- Remote work risk training and education that must be completed before providing remote access.
- Access to the Company's network through the use of VPN, in a unique, personal, and non-transferableway.
- Availability of email, instant messaging, audio / video, and collaboration tools to send or receive information and collaborative work.

Security Operations

Cencosud has processes, activities, and services to avoid interruptions of IT systems and cyber-attacks, as well as, to react appropriately to their occurrence. Here are some examples:

- 24/7 proactive monitoring throughout the year
- Technical analysis support and threat response
- Automated solutions
- Forensic analysis of digital media and electronic devices.
- Detection and mitigation of malware
- Detection and monitoring of network and host intrusions
- Assessment of emerging technological threats
- Regional / global management of cybersecurity incidents

Incident Management

In the event of incidents, the internal incident management procedure is activated.

Management and response processes for cybersecurity operations incidents:

- Coordinate cyber security incidents to ensure that all required tasks are completed, and duplicate orcontradictory efforts are avoided.
- Ensure that cybersecurity incidents are investigated in a timely manner
- Ensure that the risk associated with an incident is properly identified, measured, and controlled
- Ensure that internal notifications and required external reports are completed
- Ensure that all cybersecurity incidents are tracked centrally for trend analysis and consolidated reporting to management

Non-disclosure and confidentiality agreements

Cencosud only discloses information to third parties, if appropriate controls have been considered and implemented (as applicable) to manage the access, use and storage of Cencosud information by third parties.

These controls may include:

- Agree on confidentiality and information security obligations with the third party;
- Make appropriate evaluations of the information itself, how and why it will be disclosed; and
- Information transfer is ensured using appropriate technical or process controls as required by Cencosud to meet our legal responsibilities, customer obligations and regulatory requirements.

Supplier Security Management

Cencosud has a third-party risk management policy to identify and control the risks (including information security risks) associated with relationships and contracts with suppliers.

Cencosud requires third parties to comply with at least the same level of security according to Cencosud Group policies and standards, covering the legal and regulatory requirements that apply to Cencosud information or systems that are accessed in the provision of service to Cencosud.

In addition, third parties with access to the Cencosud network or information are subject to information security due diligence reviews based on their potential risk to the organization. Specific information security clauses are included in the terms and conditions of contracts with third parties. These may include the right to conduct audits of third-party facilities, physical and logical security controls.

Third party collaborators with access to our systems are subject to periodic access recertification.