LAVORO

PCSIC

CORPORATE INFORMATION AND CYBER SECURITY POLICY

PCSIC

CORPORATE INFORMATION AND CYBER SECURITY POLICY

CORPORATE INFORMATION AND CYBER SECURITY POLICY GRUPO LAVORO			
GROUP MONTH / YEAR	**VERSION**	**CONFIDENTIALITY**	**DESCRIPTION**
August 2023	Versão 1.6 COMPLETE	**Public Document**	Nº POL-SEG-001
March 2024	Versão 1.7 Complete	**Public Document**	Nº POL-SEG-001
September 2024	Versão 1.8 Complete	**Public Document**	Nº POL-SEG-001

Table of Contents

1 INTRODUCION

The Corporate Information and Cyber Security Policy is maintained and disseminated by the Lavoro Agro Holding Group ("Lavoro Group") to guide its employees and service providers on how to adequately protect the information handled in the exercise of their functions. All information of the Lavoro Group, its clients, employees, service providers, shareholders, and other interested parties must be obtained, handled, stored, and, eventually, destroyed according to the determinations of this policy. The determinations contained herein reflect the vision, mission, and values of the Lavoro Group, as well as the commitment of the Executive Committee on Information Security and Data Privacy to the protection of the company's information or under its custody, in accordance with Brazilian legislation and best market practices.

2 OBJECTIVES

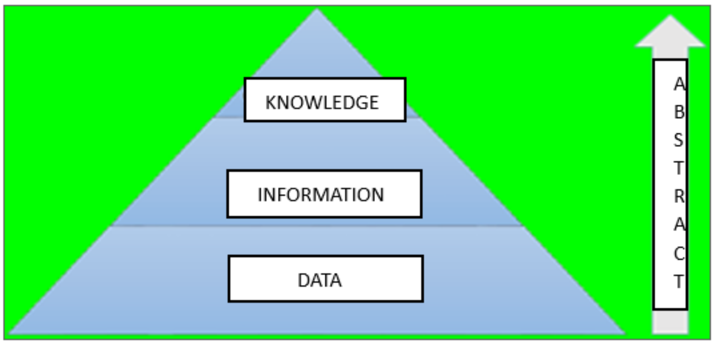
General Objectives:

To assist in the mission and vision of the organization, as well as to apply the values and ensure compliance with the company's legal and image requirements regarding Information and Cyber Security.

Specific Objectives:

- Ensure the applicability of the security policy to all employees, partners, providers, visitors, or any other agents in contact with the company's information;
- Maintain sensitive information, especially confidential client information, under the necessary and required confidentiality by established confidentiality agreements;
- Apply the culture of information security to all employees and third parties, providing through its standards and accessory procedures sufficient knowledge to recognize and avoid cyber-attacks;
- Continuously improve information security within the company.

3 TERMS AND DEFINITIONS



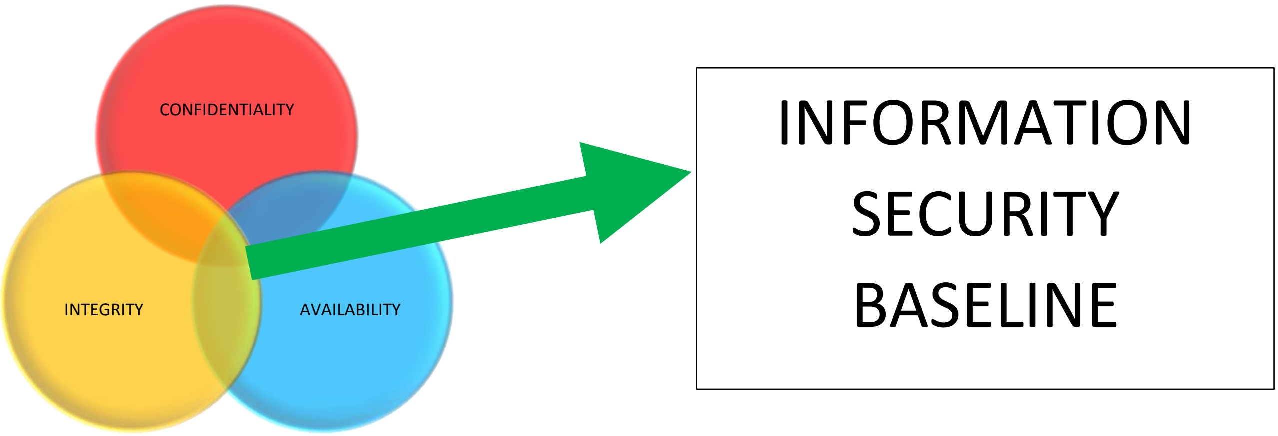
Information security is based on some fundamental principles described below:

- **Data:** It has no relevant meaning and does not lead to any understanding. It represents something that has no sense in isolation.
- **Information:** An organized set of data for forming understanding in a context.
- **Confidentiality:** The ability to keep data or information secure and available only to those who should have access. The password to a personal bank account is information that must be confidential (accessible only to the account holder).
- **Integrity:** The ability to ensure that data or information has not been altered without being noticed. For example, when modifying a document, the application that opens the document shows that it was altered by someone.
- **Availability:** The characteristic of making data or information accessible to those who have access when necessary.
- **Non-repudiation:** The ability to guarantee the authorship of data or information, preventing the author from denying (repudiating) the authorship.
- **Information Owner:** Represents someone who has ownership and rights over data or information. Often, the information owner is the company itself, with the employee or custodian.

Custodian: Represents someone who has the responsibility of handling data or information at a given moment. For example, an employee responsible for updating customer records. When they have access to the data and information, they become the custodian and are responsible for maintaining CID (confidentiality, integrity, and availability), as well as any applicable sanctions in case of non-compliance.

Information Security: Encompasses the assurance of the concepts of confidentiality, integrity, availability, and others (such as non-repudiation) for both data and information.

.



Information is one of the main assets of the institution. Thus, the Lavoro Group defines the corporate strategy for information and cyber security to protect the integrity, availability, and confidentiality of information. This strategy is based on detection, prevention, monitoring, and response to incidents and strengthens the management of cyber security risk and the construction of a robust foundation for the digital future of the Lavoro Group. To achieve this goal, we use the expanded perimeter protection strategy. This concept considers that information must be protected regardless of where it is, whether internally, in an affiliate, in a service provider, or in an international unit, throughout its life cycle, from collection to disposal.

4 RESPONSIBILITIES

All employees and third parties to whom this policy applies are responsible for the application and maintenance of information security in the company.

- **Common responsibilities for all (including employees, third parties, and visitors):**
    - Apply all items contained in this policy and other auxiliary documents;
    - Take care of the company's information and resources;
    - Report security incidents through the correct channels.
- **Senior Management:** Support this document, as well as any initiatives appreciated by the Information Security and Data Privacy Committee or any other group or individual for the purpose of applying this security policy.

- **Information Security and Data Privacy Committee / Information Technology:**
    - Establish and maintain an Information Security Management System, under which this Security Policy is supported;
    - Assist in defining and operating the necessary controls for compliance with this information security policy. For example: firewall, antivirus, access credentials, encryption, etc.;
    - Appreciate relevant company matters regarding Information Security and standardize appropriate treatments.

5. SCOPE IN SYSTEMS AND COMPUTATIONAL ASSETS

The premises defined in the policy are applicable to all computational data processing environments of the Lavoro Group, extending, but not limited to, all cloud services and systems, databases, operating systems, hardware, software, network devices, telephony, mobile devices, as well as third-party environments that are physically or logically integrated or connected to the Lavoro Group's environments and its technological park. The Lavoro Group bases its actions on national and international market best practices, which are:

- **ISO 27701 – Information Security Management;**
- **ISO 27002 – Information Security Policies;**

- **NIST – Cyber Security Framework;**
- **CIS – Center for Internet Security;**

-

6 GUIDELINES

The Information Security Policy must be available in an accessible location for employees and protected against alterations.
The Information Security Policy is reviewed annually by the Lavoro Group's Security area, with application in Brazil and abroad. The inclusion of guidelines or exceptions due to regulatory requirements and publication in foreign units will be identified by the unit's information security officer, who must formalize and submit the proposed guidelines or exceptions for prior approval by the Information Security and Data Privacy Committee. Adherence to this Policy and any deviations, in Brazil and foreign units, are periodically reported by the Information Security and Data Privacy Committee.

7 PRIVACY AND PERSONAL DATA PROTECTION

The Lavoro Group's policy is to respect the privacy and security of personal data it has access to. In its established processes, the Lavoro Group seeks to ensure that the processing of personal data will be done transparently, not for purposes different from or incompatible with those that justified its collection. All data and information shared by visitors, clients, employees, and partners on the Lavoro Group's websites and applications will be received by company employees and treated as confidential, so they will not be disclosed to third parties, free of charge or for a fee, or exposed in any way without prior consent, except under the terms of Article 7 of the General Data Protection Law (LGPD), 13.709/2018.

8 MAINTENANCE OF THE INFORMATION SECURITY POLICY

The Information Security Policy must be reviewed every 12 months. However, the Information Security Committee may initiate the review process at any time.

9 POLICIES – STANDARDS – SPECIFIC PROCEDURES

The Information Security Policy consists of its guidelines and the following standards and procedures:

- Information Classification Standard;
- Access Control and Authentication Procedure;
- Systems Operations and Management Procedure;
- Cyber Incident Management Policy;
- Vulnerability Management Policy.

10 COMPLIANCE WITH STANDARDS

It is the responsibility of every employee or service provider to ensure compliance with the Lavoro Group's Information Security Policy. In cases of knowledge of Policy deviations, possible cybersecurity incidents, information leaks affecting confidentiality, or other Information and Cyber Security standards, employees and third parties are encouraged to report to the official channel of the Lavoro Information Security area via email at security@lavoroagro.com so that preventive and corrective actions can be taken. In cases of security incidents, the IT area may, if necessary, notify employees or service providers regarding non-compliance with information security standards.

10.1 COMMUNICATION CHANNELS

- ➢ security@lavoroagro.com

11 APPROVAL

VERSION	DATA	REVIEW	RESPONSIBLE
1.8	06/09/2024	Complete revision of PCSIC where Standards and Procedures were extracted, creating accessory documents making PCSIC a unique document.	Antonio Sobrinho
1.7	26/03/2024	Revised password expiration standard and number of attempts for blocking	Antonio Sobrinho
1.6	31/08/2023	Revised LGPD and Privileged Accesses	Antonio Sobrinho
1.5	27/12/2022	Adjustments, review, and submission for approval	Fernando Cesar de Oliveira
1.4	01/06/2021	Adjustments, review, and submission for approval	Fernando Cesar de Oliveira
1.3	26/05/2021	Adjustments, review, and submission for approval	Fernando Cesar de Oliveira
1.2	26/04/2021	Adjustments	Thiago Mendes da Silva
1.1	16/09/2020	Review and alteration	Thiago Mendes da Silva
1.0	02/09/2020	**Initial Issuance**	Hubert Thomaz