Title:	**Public Policy Regarding Information Security**		
Issuing area:	**00.Corporate Policies**	**Date:**	**14/06/2024**
Code:	**PC.00.0070**	**Review:**	**2**

Summary

Title:	**Public Policy Regarding Information Security**		
Issuing area:	**00.Corporate Policies**	**Date:**	**14/06/2024**
Code:	**PC.00.0070**	**Review:**	**2**

1 – OBJECTIVE

The purpose of this document is to establish guidelines regarding the management and controls of information security and cybersecurity at Suzano, both in the Corporate and Industrial environments, to mitigate vulnerabilities, preserve and protect assets, especially information and personal data under current laws, regulations, and contract obligations, including confidentiality, integrity, availability, authenticity and legal information.

The strategic control of risks and information security is a responsibility of the **Information Security** area and must be observed by all Suzano users who process information throughout their life cycle.

1.1 - Coverage

This document is intended for all users or Service Provider Companies who process or may process information, including personal data in local or cloud assets, allocated within or outside Suzano, managed by Suzano, and/or by a Service Provider Company.

2 – REFERENCE DOCUMENTS

- Suzano's Code of Conduct;
- Lei 13.709/18 - Lei Geral de Proteção de Dados – LGPD;
- NIST Cybersecurity Framework;
- ISA/IEC 62443 - Security for Industrial Automation and Control Systems;
- NIST 800-82 - Guide Regarding Operational Technology (OT) Security;
- ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos;
- ABNT NBR ISO/IEC 27002:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.

3 – TERMS, DEFINITIONS AND ABBREVIATIONS

- **Asset:** Everything tangible or intangible that has value for the Company;
- **Authenticity:** Attribute by which it is ensured that the information was produced, sent, modified, or destroyed by a specific individual, equipment, system, authority or entity;
- **Availability:** Commitment that authorized users may gain access to information and corresponding assets whenever necessary;
- **Confidentiality:** Commitment that information is only accessible by authorized personnel;
- **Corporate Policy (PC):** Expresses the strategic direction of Suzano S.A. and permeates the entire Company;
- **Data holder:** The individual to whom the personal data being processed refers to (for example employee, former employee, interview candidate, end consumer/third parties, etc.);

- **DPO (Data Protection Officer) | Functional DPO or Data Protection Officer:** A person who supervises and provides support on all topics related to personal data processing, under applicable local and foreign personal data protection law, as well as provided in Suzano's internal policies and procedures on personal data privacy and protection, in addition to being the communication channel between the controller, data holders and the National Data Protection Authority;
- **Employee:** A category that comprises all employees, interns, and apprentices who provide services and in any way are allocated and have an employment relationship with Suzano;
- **Home Office:** Refers to non-traditional work environments, meaning all forms of work outside the office, such as teleworking, virtual work, flexible work, hybrid work, etc.;
- **Industrial Availability:** Commitment that the Industrial environment and its assets operate 24 hours a day, 7 days a week;
- **Information:** Processed or unprocessed data that can be used for the production and transmission of knowledge, contained in any medium, support or format;
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods;
- **Least Privilege**: The least privilege principle, also known as the principle of minimal privilege or principle of least authority required to perform the activity;
- **Legality:** Or non-repudiation, the use of computer and communication technology must be under the laws applicable in the location or country;
- **Mobile Features:** Any electronic equipment with mobility attributions outside Suzano's physical perimeter;
- **Need To Know:** Principle of access only to the data necessary to perform the function;
- **Peipedê Channel:** Suzano's Privacy and Personal Data Protection Center to respond to requests related to the exercise of rights by data holders as received by the organization (Website: https://www.suzano.com.br/suzano/transparencia/privacidade-protecao-de-dados);
- **Personal data processing:** Any operation conducted with personal data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, assessment or control of the information, modification, communication, transfer, dissemination or extraction;
- **Personal Data:** Any information related to an identified or identifiable individual, including sensitive personal data (racial or ethnic origin, religious conviction, political opinion, membership of a union or organization of a religious, philosophical, or political nature, data relating to health or sexual life, genetic or biometric data). Depending on the applicable privacy and data protection jurisdiction, personal information that reveals consumer data such as social security, driver's license, identity card or passport number, account login, banking account, debit card or credit card number together with any security or access code, password or credentials that allow access to an account, geolocation, and content of mail, email and text messages may be considered sensitive personal information, unless the company is the recipient of the communication. The concept of personal data is not limited to information that may be regarded as harmful to the individual's private and family life. The environment in which the information is contained is not relevant: the concept of personal data includes information available in any form, whether text, figures, graphics, photography, video, acoustic or any other possible means that leads to direct or indirect identification of the subject;

- **Privacy and Personal Data Protection Incident:** A personal data privacy and protection incident ("P&PD Incident") comprises any confirmed or suspected adverse event related to a breach in personal data security, such as unauthorized, accidental, or unlawful access that results in the destruction, loss, change, leakage or any form of inappropriate or illicit personal data processing, which may cause risks to the rights and prerogatives of the data holders;
- **Security Incident:** Any adverse event, or occurrence that promotes one or more actions tending to compromise or threaten the confidentiality, integrity, availability, authenticity, and legality of any of the Company's information assets;
- **Service Provider Company (EPS):** Company providing services or company providing goods-related services;
- **Suzano or Company:** Suzano S.A., its subsidiaries, and its controlled companies (jointly, "Suzano", "Company"), controlled (or control) is considered to be a company in which the controlling company, directly or through other controlled companies, holds shareholder rights that permanently ensure preponderance in corporate resolutions and the power to elect the majority of managers. For this Policy, "controlled companies" are those entities in which the Company has a direct or indirect interest of more than fifty percent (50%) of the share capital;
- **Threat:** Potential cause of an unwanted security incident that could damage a system or organization;
- **User:** Includes every Suzano employee and Service Provider Company who has an employment and/or contract relationship who, within the scope of this relationship, processes or may process information, including personal data;
- **Vulnerability:** Weakness in an asset or control mechanism that one or more threats can exploit.

4 – GUIDELINES

4.1 - General Guidelines

The guidelines relating to the **Information Security** area mentioned below must be complied with by all users, in all Suzano contexts. Information, including personal data, must be used exclusively for the Company's interests and each user must have restricted access to information and resources to which they are duly authorized.

The information security controls implementation must be observed both when operating in Suzano's local environment as well as in the Home Office and/or the Service Provider Company's environment, ensuring the appropriate security level for prevention and protection of assets throughout their life cycle.

4.1.1 - Logical Access Control

Logical access to information must be controlled and provided according to the responsibilities, that is, each user's role, applying the "Need To Know" and "Least Privilege" principles. Logical access accounts are non-transferable and its holders are responsible for any access.

4.1.2 - Physical Access Control

An adequate level of physical security is key to preventing and protecting access to assets controlled by Suzano, whether on its premises and/or at the Service Provider Company to inhibit unauthorized access, avoiding damage to property, business, people and information. It is also important that the premises are protected, minimizing possible risks arising from external threats, such as natural disasters, malicious attacks, accidents, among others.

4.1.3 - Information Classification

The information must be classified by its owner regarding its value for the business, sensitivity, and criticality, including by fulfilling current legal and regulatory requirements and contract obligations to avoid unauthorized modification and/or disclosure. The information owner must consider the level of confidentiality, integrity, availability, authenticity and legality, observing changes in its criticality over time and business needs.

4.1.4 - Asset Management

The existence of a single and constantly updated inventory is essential for the business and contributes to the effective protection of the assets involved. Therefore, all Suzano assets must be identified with an adequate level of detail and have an assigned owner. In addition, the identification of data sources and their respective lineages, classification, monitoring, and management of associated information throughout its life cycle must be guaranteed.

4.1.5 - Acceptable Use of Assets

Any information, including personal data controlled by Suzano, regardless of the nature of the processing: access, transmit, receive, produce, among others, throughout assets owned by Suzano and/or managed by a Service Provider Company, must only be used for professional purposes, in a lawful, ethical and moral manner.

4.1.5.1 - Mobile Resource and Home Office

For information relevant to the business not to be compromised, information security controls must be ensured for mobile and technological resources, considering the possibility of working in unprotected environments or the Home Office.

Monitoring and protection to mitigate vulnerability must be established, preventing leakage, destruction, loss or theft, change, or unauthorized access of confidential or restricted information.

4.1.5.2 - Software Installation Restriction

The use of Software not approved by Suzano is not permitted. Therefore, any type of unauthorized installation of any type of Software not licensed by the Company is prohibited.

4.1.5.3 - Intellectual Property

Technologies, intellectual works, Software, industrial designs, brands, visual identity, distinctive signs, methodologies, and any current or future information that belongs to Suzano and/or was developed, produced, created, etc., as a result of employment agreement, in any support, including on the Internet and social media, must not be used for private purposes, nor passed on to others, even if they were obtained or developed by the user in their work environment.

4.1.6 - Backup and Restore

A backup storage and recovery process of assets and information must be in place to guarantee information availability when necessary or in an event that causes any type of impact on the Company; the adoption of Backup by means of removable media, such as CD, DVD, External HD, Pen Drive, among others, is prohibited.

Backup and recovery copies must be properly tested periodically at previously defined intervals, to identify a satisfactory recovery of production environments or, in the event of an information security incident, to ensure business continuity.

4.1.7 - Malware Protection

An approved security solution that allows the detection, prevention, recovery, and eradication of all classes of malicious Software must be implemented and kept updated for Malware protection. It must be ensured that a malicious website block release list is constantly updated, or a public list is used for this purpose.

4.1.8 - Vulnerability Management

The management of vulnerabilities in local or cloud assets, allocated inside or outside Suzano, must be guaranteed through prevention actions to meet Suzano and the Service Provider Company's business needs. It is necessary to reduce the risks of cyber exposure through the identification, classification, and mitigation of vulnerabilities, avoiding impacts arising from the exploration of internal and/or external threats in the Company's environments.

4.1.9 - Information Security Incident Management

Quickly detecting an information security incident helps to reduce possible financial loss, damage to image and reputation, confidential information exposure, including personal data, business interruption, among others, in addition to controlled recovery from a security incident.

Therefore, any risk or possible information security incident must be reported immediately, through Suzano's internal or external communication channels, via email at CSIRT@suzano.com.br.

In the event of a privacy and personal data protection incident ("P&PD Incident"), it must be reported immediately through Peipedê Channel, or via email at LGPD@suzano.com.br.

4.1.10 - Risk Management

A methodology for identifying, analyzing, monitoring, and communicating information security risks must be defined and implemented, in an organized manner, ensuring the appropriate response to any risk that may impact Suzano. The process must be conducted continuously and according to the Company's needs in order to promote the most appropriate information security actions and, consequently, reduce exposure to threats and the probability of causing any type of damage to any of Suzano's tangible or intangible assets.

4.1.11 - Hardening and Patch

Hardening management must be defined and implemented to reduce the risk of asset exposure, by eliminating or limiting potential attack vectors or reducing the attack surface. The purpose is to remove unnecessary actions, including, but not limited to, superfluous configurations, standard account functions, Software, ports, permissions, and access.

Patch management must be defined and implemented for the Software's safe distribution, test, and application, that is, the security update allows the correction of vulnerabilities susceptible to cyber-attacks, in addition to ensuring adequate support, compliance with applicable laws, regulations, and contract obligations, providing resource improvements related to the Software.

4.1.12 - Traceability

Records of access events to assets considered critical and which convey information classified as confidential and restricted must be collected automatically, in a structured manner, adequately protected to avoid unauthorized modifications, guaranteeing integrity and authenticity, and must also be monitored and stored for a reasonable period, so it is available upon request.

4.1.13 - Cybersecurity

Cybersecurity must be guaranteed to promote actions aimed at operational security, through vulnerability mitigation, to ensure that assets are capable of resisting events in cyberspace, with the possibility of compromising the availability, integrity, confidentiality, authenticity, and legality of data stored, processed, or transmitted, allowing the reduction of disturbances or downtime, ensuring high availability in both the Corporate and Industrial environments, avoiding impacts for the Company.

4.1.14 - Network Security

The Corporate environment must be segregated from the Industrial environment through security solutions. Also, network segmentation must be implemented, as a network that has its services distinctly segmented becomes more secure, providing access traceability at the network level and minimizing the risk of lateral movement of threats.

4.1.15 - Security in the Service Provider Company

Minimum information security criteria must be defined to mitigate risks and protect Suzano's assets and controlled information accessible and/or managed by the Service Provider Company (EPS). The service provider is liable for the information's safe and confidential storage under the confidentiality clause

established in the contract and/or Data Processing Agreement (DPA) when it involves personal data and applicable law.

4.1.16 - Awareness and Training

The Information Security area must define a process that implements, monitors, and measures structured actions, which indicates, promotes, and supplements activities related to awareness and training in information security and cybersecurity, regularly. The purpose is to spread knowledge and qualify users to prevent and protect Suzano's assets against threats.

4.1.17 - Business Continuity Management (Resilience)

It must be ensured that minimum resources (people, processes, and technology) are preserved in a moment of disruption, allowing for a reduction in impact and resumption of Suzano's critical activities. Therefore, it is necessary to define a methodology for monitoring the main initiatives on business continuity, disaster recovery, and crisis management, through the identification and prioritization of critical functions and processes that may cause the greatest impact if they are not available.

4.1.18 - Personal Data Privacy and Protection

Everyone is responsible for ensuring the personal data protection to which they have access, including, but not limited to, protection from improper or unauthorized access. The security actions necessary to guarantee personal data security must be applied, seeking to preserve information, including personal data from third parties that may have been accessed during or after the relation established between the Service Provider Company, Third Parties, and Suzano.

It is not permitted to copy and/or share any documents, spreadsheets, agreements, or contacts of customers, Service Provider Companies (EPS), employees, and Suzano business partners containing personal data outside the context established in the agreement and internal policies, under penalty of violating the Code of Conduct and current personal data protection law.

Suzano is committed to the legitimate and lawful personal data processing of all individuals, that is, data holders who interact with us: employees, shareholders, customers, and representatives of business partners.

Personal data privacy and protection are fundamental rights and Suzano is committed to safeguarding these rights, reason why it adopts the following principles: non-discrimination, transparency, security, data quality, minimization, free access, prevention, liability, and accounting. Any personal data processing activities must always respect and ensure compliance with applicable laws and regulations, always acting with transparency and according to the purpose for which the personal data was collected.

Personal data privacy and protection must be considered throughout the life cycle of personal data, from collection, disposal, storage, sharing, and lawful use of personal data.

For more information about how personal data is processed, access the **Peipedê Channel**.

5 – RESPONSIBILITIES

Not Applicable.

6 – APPROVAL OF THE POLICY

This Policy comes into force on the date of its minimum approval by the Executive Manager of Information Technology, which is the Company's body that has exclusive competence to change, in any event, this Policy.

7 – VIOLATION OF POLICY

Violations of this policy are subject to disciplinary sanctions provided in Suzano's internal rules and in the applicable law in Brazil and in the countries where the companies are located.

8 – MISCELLANEOUS

This policy must be public. All users are liable for monitoring the updating of this policy, and it is prohibited to claim ignorance.

9 – APPENDICES

Not Applicable.