0	03	90	002

POLICIES, STANDARDS, AND PROCEDURES

Information Security Policy

1. GOAL

This policy aims to establish general guidelines and principles of information and cyber security for Cosan Group companies, in an effort to ensure that users act in compliance with the rules regarding the treatment and protection of information and information assets, as well as to ensure the ability of the Cosan Group to guarantee confidentiality, integrity, availability, authenticity, irrevocability and responsibility, as well as preventing, detecting and reducing information security and cyber risks.

2. APPLICATION AND SCOPE

It applies to all employees of the Cosan Group in Brazil and abroad, since its approval date on **11/08/2023** (MM/DD/AAAA). It covers Cosan and all subsidiaries of the Cosan Group.

Cosan Group suppliers are also subject to the guidelines, procedures and controls set forth in this policy whenever they process information or use Cosan Group's information assets.

3. DEFINITIONS

- **Collaborator**: employees, contractors, subcontractors, interns, apprentices and administrators;
- **User**: any individual, process, device or mechanism that accesses, uses or manipulates an information or information asset;
- **Supplier**: supplier companies, partners and service providers to third parties that have entered into a supply, partnership and/or service contract with the companies of the Cosan Group, as well as their representatives, employees and subcontractors;
- **Cyber Defense Center (CDC):** Team composed of professionals that aims to monitor and protect the Cosan Group against digital threats;
- **IT**: Information Technology;
- Logging: technical term used to describe the record of transactions that occur when software is used;
- **Database**: organized collection of structured information - or data - usually stored electronically in a computer system;

- **Software development**: activity of creating computer programs, performed by a developer or group of developers;

- **Personal Data**: any data that relates to an identified or identifiable individual or a person who can be identified by means reasonably likely to be used. For example, the following are considered Personal Data: name, age, gender, affiliation, physical and electronic address, document numbers, corporate identifiers ("CS" and "TR"), electronic identifiers (IP, IMEI), geolocation, internet browsing profile and consumption profile.

- **Sensitive Personal Data**: personal data on racial or ethnic origin, religious belief, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, which is linked to a natural person.

- **Software**: logical part, the set of instructions and data processed on servers and computers. All interaction of computer users is carried out through software;

- **Malware**: variety of forms of hostile or intrusive software that can cause damage to the technological environment;

- **Spyware**: spy software that is usually installed on the phone or computer without the user's consent;

- **Botnets**: network of computers that have been infected by malicious software and can be controlled remotely to perform malicious attacks;

- **VPN**: from English, virtual private network. Technology that allows remote access to the corporate network.

4. PRINCIPLES OF INFORMATION SECURITY

Information security covers 5 (five) fundamental pillars, highlighted below:

- **Confidentiality:** Ensures that information and information assets are accessible only by authorized users, for the necessary period;

- **Availability**: Ensures that information and information assets are available to authorized users whenever necessary for business processes or customers;

- **Integrity**: Ensures that information and information assets are complete and intact and that they

have not been modified or destroyed in an unauthorized or accidental manner during their life cycle;

- **Authenticity**: Guarantees the ownership of the information and that it comes from the advertised source and has not been subject to undue changes throughout an established process.

- **Irrevocability (non-repudiation)**: Ensures that a person or entity cannot deny authorship of the information provided, as in the case of the use of digital certificates for online transactions and signature of electronic documents. In information security management, this means being able to prove what was done, who did it and when it did it in a system, making it impossible to deny users' actions.

4.1 GENERAL ASPECTS

a. The protection of the information and information assets of the Cosan Group must be a constant priority in all business and support areas, in order to reduce risks, as well as damages and/or losses that may compromise the image and organizational objectives;

b. The protection of information and information assets must be applied in a manner compatible with its impact on the Cosan Group, covering all processes, computerized or not. The information under the responsibility of the Cosan Group must be handled in accordance with current laws and internal procedures and used only for the purpose for which it was collected, avoiding the compromise of its confidentiality, integrity, availability and authenticity, including, but not limited to, when using external solutions, platforms and resources, such as: messaging applications, social networks, artificial intelligence applications, etc. The employee is responsible for actions taken in the treatment of data owned by the Cosan Group and/or third parties entrusted to him by virtue of his professional activity, throughout his life cycle. Thus, it ensures that the person responsible answers for such questions, including before the law;

c. A person or entity cannot deny the authorship of the information provided, therefore, irrevocability guarantees the authenticity of actions taken under a particular user or process;

d. If applicable, and whenever possible, the processes of the Cosan Group shall ensure the segregation of functions through the participation of more than one employee or team of employees in the activities, in order to avoid conflict of interest and reduce the risk of accidental or purposeful misuse of information assets and systems;

e. All employees and suppliers of the Cosan Group, as applicable, should be aware that the use of information assets, systems and environments, and their password policies, may be

monitored and that the records may be used to detect violations of this Policy and information security procedures, serving as evidence for the application of disciplinary measures, administrative and/or legal proceedings;

f. Information security risks, as well as questions about the Policy and related procedures should be reported to the Corporate Information Security area and/or to the local information security representative (Business Information Security Officer – BISO);

g. Except with the express authorization of their responsible owner, the technologies, brands, methodologies and any information of the Cosan Group shall not be passed on or shared with third parties, as well as for personal purposes, even if they have been obtained or developed by the employee himself during the exercise of his functions.

5. GUIDELINES, CONTROLS AND PROCESSES

5.1 SECURE USE OF IT RESOURCES

Corporate resources, according to the internal procedure "Safe use of IT resources", should only be used for professional purposes, and the companies of the Cosan Group have the right to control and monitor the use of resources provided to employees and third parties.

5.2 CLASSIFICATION OF INFORMATION

Where applicable, all information created must be classified and protected throughout its life cycle, in accordance with the Information Classification Procedure. The information lifecycle comprises its creation or collection, handling, storage, transportation, and disposal.

To ensure adequate protection of information, it must be classified according to its value, legal requirements, relevance, sensitivity and criticality to the Cosan Group. The classification criteria should consider business needs, regulatory demands, sharing or restriction of access, and the impacts in the event of misuse of information.

Below are the recommended levels of secrecy (Public, Internal, Confidential and Restricted). However, Cosan Group companies may establish their own labels as long as they are comparable to those listed in this Policy, according to the internal procedure "Classification of Information".

The classification of the information (level of secrecy) is the responsibility of the area that generated it.

a. **Public Information:** may be made available without restriction. The knowledge of this information

by any individual does not impact the Company's objectives.

b. **Internal Information:** can only be made available to the users of the Company. Information of this level of secrecy is operational and its knowledge by third parties does not impact business objectives.

c. **Confidential Information:** indicates strong restriction on misuse and access. It can lead to financial, operational impact or loss of competitive advantage. When misplaced or misused, it can seriously damage business objectives. The manager in charge shall explicitly indicate which functions may have access.

d. **Restricted Information:** information whose use and access are restricted to a specific group of nominally designated collaborators, and may not be disclosed to unauthorized persons, in whole or in part, in any format. It comprises subjects, documents, images, or any strategic, highly sensitive and critical materials. Their unavailability, unauthorized disclosure or alteration causes serious damage to business objectives.

5.3 PROTECTION OF PERSONAL DATA AND SENSITIVE DATA

The Cosan Group takes seriously the protection of personal data and sensitive data and the security measures established in this Policy are essential to ensure compliance with the legislation on the protection of personal data (LGPD).

To comply with the terms of this Policy and the Privacy and Data Protection Policy, the Cosan Group establishes the Privacy and Data Protection Program.

5.4 CYBER SECURITY

In order to assist in the implementation of the guidelines established in this Policy and the controls, processes and procedures of the Information Security and Cybersecurity Management System of the Cosan Group, the best practices available in the market are adopted by default:

a. Authentication measures capable of individualizing users who access information assets, systems and environments of the Cosan Group;

b. Use of encryption, masking and obfuscation, where applicable, for the storage of relevant and sensitive information, including personal data, in information assets, systems and environments of the Cosan Group and suppliers;

c. Solutions for the prevention and detection of intrusion and unauthorized access to the information

assets, systems and environments of the Cosan Group;

d. Use of procedures and controls to prevent information leakage;

e. Periodic tests and scans to detect flaws and vulnerabilities in the procedures, controls, systems and environments of the Cosan Group;

f. Protection solutions against malicious software (*malware, spyware, trojans*, viruses, *botnets*, etc.) that can affect information assets, systems and environments of the Cosan Group;

g. Activity tracking systems and logs for activities carried out by the Cyber Defense Center (CDC);

h. Access control of users who make use of the Cosan Group's systems and environments;

i. Segregation and segmentation of the different network environments made available by the Cosan Group or suppliers contracted by it to its employees, suppliers and customers, when applicable and validated by the Information Security area;

j. Maintenance of backups of information;

k. The minimum controls listed should also be applied in the development of new products, solutions, applications, systems and environments, as well as in the acquisition of new technologies and services that will integrate operational activities. Likewise, the minimum controls listed shall also be adopted, as applicable, by suppliers who process or store sensitive or relevant information for the conduct of the Cosan Group's operational activities.

5.5 IDENTITY AND ACCESS MANAGEMENT

The processes of granting, altering and deleting access to the information assets, information systems and/or environments of the Cosan Group are carried out by the competent area upon formal approval of the applicant's manager and the respective owner of the system and/or profile, whenever necessary for the performance of the activities, according to the internal procedure "Identity and Access Management".

5.6 USE OF PASSWORDS

The password is the responsibility of each employee, who must consider minimally the following rules:

a. The password is personal and non-transferable;

b. The use of corporate passwords on computers and mobile devices not approved by Grupo Cosan is expressly prohibited;

c. Password storage in web browsers should be avoided;

d. Passwords should not be written down or stored in physical and digital media (e.g., email, spreadsheets, notepad, files on the network, etc.);

e. Different passwords should be used for different services. Private-use passwords must be different from corporate passwords;

f. If the employee suspects that the password has been discovered, they must request a change and/or immediate block;

g. It is forbidden to use the name of any company, products or services of the Cosan Group, and sequential numbers in the formation of the password.

5.7 ASSET MANAGEMENT

The inventory of IT assets needs to be maintained and constantly updated contemplating the main information assets, such as: systems, applications, databases and servers.

Hardware should be purchased only from approved vendors, and maintained with the following guidelines in mind:

a. Only approved software configurations should be applied to new hardware;

b. End users should take due care with any hardware that has been delivered to them;

c. Lost and/or stolen hardware must be reported immediately to the competent Service Desk or IT area;

d. End-of-life hardware should be disposed of safely, according to the guidance of the Service Desk or competent IT area.

5.8 RISK MANAGEMENT IN INFORMATION SECURITY

The Cosan Group has a structured process of monitoring, analysis and identification of risks, vulnerabilities, threats and impacts on information assets, so that appropriate controls and effectiveness are periodically tested, as referenced in the procedure "Risk Management in Information Security".

5.9 INFORMATION SECURITY INCIDENT MANAGEMENT

The Cosan Group adopts specific procedures, requirements and controls for the detection, treatment and response to incidents that have occurred, in accordance with the "IT & OT Incident Response Procedure".

The procedures, controls and requirements for suppliers must be aligned with the Cosan Group's own levels of complexity, comprehensiveness and accuracy.

5.10 INFORMATION SECURITY TRAINING AND AWARENESS

As part of its commitment, the Cosan Group adopts actions and initiatives to promote the training, acculturation and evaluation of employees on the subject of information security, reinforcing the guidelines stated in this policy.

5.11 INFORMATION SECURITY ASSESSMENT IN THE CONTRACTING OF SERVICES

The processes and controls necessary to reduce the risks associated with outsourcing initiatives, including cloud computing agreements, should be part of the business agreements between suppliers and Cosan Group companies.

The companies of the Cosan Group reserve the right to assess whether the supplier meets the information security requirements, based on standards, good market practices and the procedure "Information Security Risk Assessment in Suppliers".

Contracts with third parties must ensure that the staff or subcontractors of the external organization comply with the Cosan Group's regulatory information security documents.

5.12 ACQUISITION, DEVELOPMENT AND MAINTENANCE OF SOFTWARE

The software acquisition process must respect all computer software copyrights and the terms of all software licenses to which the Cosan Group companies are a part.

Cosan Group companies must manage their software assets and ensure only the use of legal software on their workstations and servers.

Copies of third-party software, copyrighted by the software developer, unless expressly authorized, are prohibited under the Safe Use of IT Resources procedure.

Systems and applications developed internally or by specification of Cosan Group companies must comply with the "Secure Systems and Application Development Procedure" and ensure:

a. Privacy impact assessment must be completed for major software changes;

b. Software security requirements should be documented as part of the development process;

c. Software changes must be subject to control procedures;

d. Only authorized users are allowed to deploy software changes ;

e. Guarantee of segregation of duties concept for both business activities and IT administration;

f. Authentication assurance and security configuration for access passwords;

g. Segregation of environments for development, quality and production;

h. The contracting of services for maintenance and development of applications should contain security requirements (e.g. using an RFP template or specific document for hiring);

i. Assurance of security assessment in code prior to promotion to productive environments.

6. DISCLOSURE OF THIS POLICY

This policy is disclosed to all employees of the Cosan Group and is available on the communication channels of each company (e.g. Intranet, Knowledge Library in Workplace, POC etc.).

7. DISCIPLINARY MEASURES

The suspicion of non-compliance with the procedures of this Policy by employees or third parties will be determined by the competent Committees and evaluated by the Board of Directors or equivalent, as provided for in the internal investigation procedure.

Employees who may be violators will be subject to the disciplinary sanctions provided for in the Disciplinary Measures Policy and the Code of Conduct, without prejudice to Cosan adopting the appropriate administrative, civil and criminal measures as the case may be.

Third parties who may be violators will be subject to the applicable contractual commercial sanctions, including the immediate termination of the contract, with the application of the penalties arising from the termination, without prejudice to indemnification action and other applicable legal measures.

8. REPORTING AND QUESTIONS

It is the responsibility of all employees and third parties to ensure compliance with this Policy.

0	03	90	002

Indications of non-compliance or doubts about compliance with this Policy or the Code of Conduct may be reported to the employee's immediate manager, the Human Resources department, Internal Audit, Compliance or through one of the available Communication Channels (0800-725-0039 or www.canaldeetica.com.br/cosan).

Cosan does not tolerate any retaliation against any person, internal or external, who reports in good faith a violation or suspected violation of this Policy or its Code of Conduct, and confidentiality about the identity of any person who reports any violation is guaranteed.

The practice of retaliation is subject to disciplinary measures that may result in the termination of the Cosan employee or termination of a contract, as the case may be.

9. REVIEW OF THIS INFORMATION SECURITY POLICY

This Policy must be reviewed at least once a year, and any changes must be approved by the Board of Directors.

10.REVIEW AND APPROVAL

Stage	**Name**	**Position/Function**	**Revision**
Elaboration	Thiago Kysyk Nogueira Field	Information Security Coordinator	Version 2
Revision	Andre Novaes Frutuoso	Information Security Manager	
Approval	Fernando Madureira	Director of Cyber Information Security (CISO)	
Elaboration	Cristiane Belitardo Pagoti de Britto	Information Security Analyst	Version 1
Revision	Andre Novaes Frutuoso	Information Security Manager	
Revision	Wagner of Cicco	Head of Audit and Internal Controls	
Approval	Fernando Madureira	Head of Information Security (CISO)	