Alupar

Policy

Information Security and Cyber Security

Code: HO-TIN-PL-002 | First version: 28/07/2017 | Last version: 07/2025

1. Objective

This document aims to establish the guidelines and responsibilities regarding the protection of information at Alupar Investimento S.A. ("Company"). These guidelines serve as the basis for the norms, standards, and procedures that regulate the objectives defined herein as important for good Information Security management practices.

Alupar Investimento S.A.'s Information Security and Cybersecurity Policy directs requirements for maintaining the Integrity, Availability, Confidentiality, Authenticity, and Privacy of the Company's information and/or information under its custody.

The guidelines established in this document observe and comply with the applicable legislation on Personal Data Protection, especially Law No. 13,709/2018 and its subsequent amendments ("Lei Geral de Proteção de Dados Pessoais" or "LGPD"), as well as the Company's internal Personal Data Protection policy.

This document is valid until 07/26

2. Scope and Applicability

Aplica-se This text applies to all information within the technological and conventional environments of Alupar Investimento S.A. and/or companies in which it holds direct or indirect participation ("Companies"). Its target audience includes the entire management structure and collaborators, including employees, interns, suppliers, service providers, and business partners, who at any point have access to the Companies' environment and proprietary information, processed on the Corporate and Operational networks.

3. Dictionary

Threat - A potential cause of an unwanted incident, which may result in damage to the Company.

Asset - Anything (e.g., IT assets, computers, mobile devices, systems, applications, information, etc.) that has value to the Company and needs to be adequately protected.

Intangible Asset - Any element that holds value for the Company, existing in digital format or as an abstract, yet recordable or perceptible entity. This includes, but is not limited to, data, reputation, image, brand, and knowledge.

Authenticity - Assurance that information is genuine and reliable, providing non-repudiable evidence of the identity of the entity that created, edited, or issued it.

Collaborator - Individuals encompassing senior management, employees, interns (in accordance with Intern Law – Law 11,788/2008), young apprentices (in accordance with Apprenticeship Law – Law 10,097/2000), outsourced service providers, and contractors of the Company.

Confidentiality - A principle tied to information privacy. It guarantees that the Company's data will not be made available or disclosed to unauthorized individuals, entities, or processes.

Availability - The property of ensuring information is accessible and usable by authorized users when required.

Security Incident - Any adverse event, confirmed or suspected, related to information system security, leading to the compromise of one or more basic Information Security principles: confidentiality, integrity, availability, and authenticity. Examples include: computer intrusions, denial-of-service attacks, information theft by internal personnel and/or third parties, data leakage/breach, misuse of privileged access, and unauthorized or illegal network activities.

Information - A strategic and high-value asset for the Company, owned by it or under its responsibility, which must be protected in compliance with current legislation, ethical values, and information security best practices.

Integrity - Assurance that information is maintained in its original state, ensuring its protection against unauthorized, intentional, or accidental alterations during storage or transmission.

Non-repudiation - Assurance that the sender of any data or information, or the author/initiator of any action regarding information, cannot subsequently deny having sent the data/information or having performed that action.

Incident Response – A pre-defined process that describes how the Company should handle an Information Security or Cyber incident.

Risk – The possibility of an event occurring, which can be a Threat (when negative) or an Opportunity (when positive).

Cyber Security - The practice of employing a set of means and technologies to defend information systems, infrastructure, computer networks, and/or personal devices. It aims to prevent damage, theft, intrusion, alteration, or destruction of information caused by cyber attacks, and is fully encompassed by this Policy.

Information Security - The preservation of information's properties, notably its confidentiality, integrity, availability, and authenticity. This enables the controlled use and sharing of information, regardless of the medium used for its storage, processing, or transmission.

Third Parties - Any natural person or legal entity engaged to obtain and/or retain business, including but not limited to advisors, consultants, subcontractors, sales representatives, and joint venture partners; or engaged to represent the Companies or their interests before a government, a state entity, a state-owned enterprise (SOE), or a state-controlled entity. This also includes all service providers and suppliers.

User - Any Collaborator or Third Party who utilizes the Company's IT resources.

Violation - Any activity that violates the rules established in the Company's internal policies and procedures.

4. General Guidelines

The guidelines established in this Policy aim to:

Protect the Company's value and reputation;

Ensure the confidentiality, integrity, and availability of the Company's information and Third-Party information under its custody. This includes protecting against unauthorized access and modifications, and ensuring that information is available to all authorized parties when necessary;

Identify Information Security violations, implementing systematic actions for incident detection, response, and prevention;

Alupar

Ensure the Company's business continuity, protecting critical processes from unacceptable interruptions caused by significant failures or disasters;

Comply with legal, regulatory requirements and contractual obligations pertinent to the Company's activity;

Raise awareness, educate, and train Users on Information Security policies, norms, and procedures so they can be applied to their daily activities;

Establish and continuously improve the Information Security and Cybersecurity Risk Management Process;

Ensure that personal data is not lost, stolen, misused, or leaked by unauthorized users;

Establish controls for data loss prevention, aiming to mitigate common risks through the establishment of governance mechanisms, and the continuous evaluation and improvement of all specific aspects of personal data privacy and protection.

5. Responsibilities

5.1 Directorate

- Demonstrate commitment to promoting strategic guidelines, provided they are previously aligned with the Company's Board of Directors, as well as in relation to responsibilities, competencies, and support for the Information Security Management System (ISMS), in order to ensure the protection of its tangible and intangible Assets.

- Submit for analysis to the Information Security Committee any and all matters involving strategic themes or risk assumption, concerning Information Security.

5.2 Information Security Management

- Ensure that all Information Security-related matters are handled in a consistent and effective manner, establishing an information security culture and awareness among all Company Collaborators;

- Develop, safeguard, maintain, and disseminate this policy, as well as other pertinent Information Security and Cybersecurity policies and standards that complement this policy;

- Review all Information Security and Cybersecurity related policies at least once a year, updating as necessary to reflect changes in business objectives or the Company's environment;

- Seek support and guidance regarding legal aspects related to contracting processes and legislative and regulatory requirements concerning Information Security.

5.3 Information Security Committee

- Ensure that all matters related to Information Security and Cybersecurity are addressed consistently and effectively, establishing a culture and awareness of Information Security and Cybersecurity among all Company Collaborators;

- Evaluate and approve all security policies at least once a year, updating as necessary to reflect changes in business objectives or the Company's environment;

- Evaluate, monitor, and deliberate on matters related to Information Security and Cybersecurity, considering the Company's risk strategy;

- Submit for analysis to the Governance Committee, Audit Committee, and for subsequent deliberation by the Board of Directors any and all matters involving strategic themes or risk assumption, with regard to Information Security and Cybersecurity.

- Ensure the accountability of Collaborators and/or Third Parties who fail to observe the Companies' internal policies and procedures related to Information Security and Cybersecurity.

5.4 Information Technology Department

- Define and implement procedures for the secure configuration of the Company's technological environment;

- Maintain records of all security violations that occur in the Company's environments and systems, containing sufficient detail for them to be used in disciplinary actions and/or for the review of policies and procedures;

- Monitor and analyze security alerts and information, distributing them to the appropriate teams for handling, in accordance with the requirements and procedures defined in the Incident Handling and Response Standard;

- Administer User accounts, including additions, deletions, and modifications, continuously evaluating the management of authentication to system components;
- Ensure that Collaborators have access only to previously authorized information and resources;
- Perform periodic evaluations of User accounts and access controls to ensure their validity and accuracy;
- Implement, administer, and monitor technology and security controls that support, verify, and evidence the application of this Policy.

5.5. People Management

- Conduct the awareness program and provide periodic training with the support of the Information Security area;
- Ensure the availability of Information Security documents to all Company Collaborators;
- Ensure that, during the onboarding process, Collaborators receive orientation on Information Security and Cybersecurity.

5.6 Managers

- Manage and ensure compliance with this Policy and other complementary documents by its Collaborators;
- Ensure that contracts and services under its responsibility adhere to this Policy and other complementary documents;;

- Carefully evaluate before approving access requests for Collaborators to the Company's information and resources, specific systems, or applications. This evaluation must ensure that granting permissions does not compromise the Company's information security by exceeding the needs of the work activities performed, in adherence to the Principle of Least Privilege (minimum necessary accesses and authorizations for the execution of duties);

- Inform the Human Resources Management area and the Information Security Management about any changes in access rights, transfers, and changes in roles for Collaborators under their responsibility;

- Ensure that its Third Parties are knowledgeable of this Policy and its complementary standards.

5.7 Employees

- Protect the Company's information according to its classification and sensitivity. In the absence of a label or explicit classification, no proprietary information or information under the Company's responsibility may be disclosed without prior and formal authorization from the Information Security area;

- Know and follow all Company security policies and operational procedures that are pertinent to their functions and activities;

- Understand their responsibilities regarding Information Security and Cybersecurity, acting in a secure, ethical, and legal manner when using the Company's resources and data, prioritizing the preservation of the confidentiality, integrity, and availability of the Company's information;

- Be held accountable for damages caused due to non-compliance with the rules for protecting information and computational resources of the corporate network, as stipulated in this Policy;

- Participate in the corporate Information Security and Cybersecurity awareness program and training;

- Safeguard any and all information stored on the corporate network against unauthorized alteration, destruction, disclosure, copying, and access;
- Ensure the proper use of hardware resources and their conservation for professional activities, both their own and their colleagues';
- Maintain the confidentiality of confidential information, keeping it restricted;
- Maintain the confidentiality and non-transferability of passwords for accessing the organization's computational resources;
- Formally report to their Manager any events related to the violation or potential violation of this policy or any suspicious activities;
- Comply with pertinent recommendations contained within the Company's information security policies and procedures.

6. Accession

Adherence to this Policy implies strict observance of the rules contained herein and in applicable legislation, under penalty of disciplinary sanctions. Collaborators' adherence to this Policy will be formally confirmed through the signing of the "Term of Adherence to the Information Security and Cybersecurity Policy".

Collaborators will be notified whenever changes made to this Policy are considered relevant and/or imply additional obligations. Thus, Collaborators must reiterate their adherence to the Information Security and Cybersecurity policy and standards.

7. Disciplinary sanctions

Any activity that disregards the guidelines established in this Policy will be considered a violation and handled by the Information Security area, in order to ascertain the responsibilities of those involved, aiming for the application of disciplinary measures and/or applicable sanctions stipulated in contractual clauses and current legislation by the responsible areas.
Any detected attempt to circumvent the established guidelines and controls will be treated as a violation.

8. References

- Term of Responsibility;
- Code of Ethics, Conduct & Compliance;
- Privacy Policy;
- Complementary Information Security Standards;
- ABNT NBR ISO/IEC 27001:2013 Standard;
- ABNT NBR ISO/IEC 27002:2013 Standard.

9. Regulatory Foundations

- Law No. 9,609/98 (Software Law);
- Law No. 9,610/98 (Copyright Law);
- Law No. 13,709/2018, the LGPD;
- Law No. 12,965/2014, the Internet Civil Framework;
- Law No. 12,527/2011, the Access to Information Law;
- Regulations and norms published by the ANPD (National Data Protection Authority);
- Constitution of the Federative Republic of Brazil, of October 5, 1988;
- Federal Law 8,159, of January 8, 1991 (Provides for the National Policy on Public and Private Archives);
- Federal Law 9,279, of May 14, 1996 (Provides for Trademarks and Patents);
- Federal Law 3,129, of October 14, 1982 (Regulates the Granting of Patents to authors of industrial inventions or discoveries);
- Federal Law 10,406, of January 10, 2002 (Establishes the Civil Code);
- Decree-Law 2,848, of December 7, 1940 (Establishes the Penal Code);
- Federal Law 9,983, of July 14, 2000 (Amends Decree-Law 2,848, of December 7, 1940 - Penal Code and makes other provisions);
- Decree No. 9,637, of December 26, 2018 - National Information Security Policy.

10. Revision History

Revision Number	Date (mm/yyyy)	Review Description	Approver
01	07/2017	Document creation	-
02	02/2023	Review based on the IS Project and update with ISO 27001	Alupar Board of Directors
03	07/2025	Periodic review	Alupar Board of Directors

This Policy may be amended at any time, without prior notice.