	CORPORATE POLICY	Code	
cba	Information Security Policy Summary	Version	
		Department	Information Security
		Phase	Effective

- The Information Security Policy of Companhia Brasileira de Alumínio (CBA) aims to establish standards and guidelines to safeguard information and information technology resources. This Policy applies to all employees, interns, contractors, third parties, suppliers, other related parties, and their controlled entities.
- Senior Management is responsible for promoting the information security strategy and ensuring the resources necessary for the implementation, maintenance, and continuous improvement of the Information Security Management System (ISMS), to keep pace with the evolution of risks, threats, and business needs.
- The Information Security department, led by CISO Samuel Cavalcante, develops security plans, implements preventive and corrective measures, coordinates risk and incident management, monitors threats and vulnerabilities, prepares and tests disaster recovery plans, and promotes an information security culture throughout the Organization.
- The Organization continuously monitors cybersecurity risks and adopts measures to prevent, detect, respond to, and mitigate information security incidents. When applicable, it maintains appropriate communication with affected stakeholders, observing legal, regulatory, and contractual requirements, as well as the actions taken to reduce impacts and prevent recurrence.
- Information security is a responsibility of the entire Organization. All users, including employees, interns, and contractors, must comply with the Policy, adequately protect information, report suspected violations, vulnerabilities, or security incidents, and participate in awareness programs and training promoted by the Organization.
- Information must be classified according to sensitivity and criticality levels. Safe behavior and responsible use of information are mandatory to preserve its confidentiality, integrity, availability, and protection against unauthorized access, changes, and disclosure.

- The Information Security Policy will be reviewed annually or whenever significant changes occur in the information security environment, with approval from Senior Management and communication of changes to the relevant audiences. Non-compliance with the guidelines established in this document will result in disciplinary measures or applicable sanctions, according to the nature of the relationship with the Organization.