Eletrobras

ELETROBRAS COMPANIES INFORMATION SECURITY POLICY

Version 5.0
12/01/2022

Eletrobras Companies Information Security Policy

Area responsible for issuing

Board of Governance, Risks and Compliance / Superintendance of Risk Management, Internal Controls and Information Security.

Target audience

Employees of Eletrobras companies who may have access, directly or indirectly, to corporate and operational information and technology resources.

Approval

Resolution RES-501/2022, of 24/10/2022, of the Eletrobras Executive Board of Directors
Deliberation DEL-168/2022, of 01/12/2022, of the Board of Directors of Eletrobras.

Repository

The policies of Eletrobras companies can be found on the website:
https://eletrobras.com/pt/Paginas/Estatuto-Politicas-e-Manuais.aspx

Copyright and confidentiality

Maximum review period: 3 years.

Issue history:

Editing	Approval	Main changes
1.0	RES-833/2017, of 12/26/2017 and DEL-008/2018, of	Does not apply.
2.0	RES-677/2018, of 09/25/2018 and DEL-200/2018, of	Inclusion of the guidelines of the Eletrobras Companies SAP Access Control Policy, at the request of the Audit and Statutory Risks Committee (CAE).
3.0	RES-251/2021, of 04/19/2021 and DEL-079/2021, of	Expansion of references, concepts and values present in the General Data Protection Law (LGPD) and the Decree on the National Cybersecurity Strategy. Withdrawal of the Appendix for transformation into a
4.0	RES-076/2022, of 03/07/2022 and DEL-037/2022, of	General review of the document, resulting in corrections and adjustments of content to meet the demand of the Operational Technology Committee of Eletrobras Companies (CTOEE), with the objective of encompassing information security specifications for Operational Technology (OT).
5.0	RES-501/2022, of 10/24/2022 and DEL-168/2022, of	Necessary adjustments due to the change in the legal nature of Eletrobras companies, in relation to legal references and classification of information.

Summary

1 Objective

Strategically guide issues related to information security, defining guidelines for the protection, preservation and disposal of information in the conventional or technology environment of Eletrobras companies.

2 References

2.1 Law No. 13,709 of August 14, 2018 - General Data Protection Law (LGPD).

2.2 Decree No. 10,222 of February 5, 2020 - Approves the National Cybersecurity Strategy.

2.3 Decree No. 9,637 of December 26, 2018 - Institutes the National Information Security Policy, provides for information security governance.

2.4 Decree No. 3,505/2000 - Establishes the Information Security Policy in the bodies and entities of the Federal Public Administration.

2.5 GSI/PR Ordinance No. 93, of October 18, 2021 - DOU [Federal Official Gazette] - National Press (in.gov.br).

2.6 Aneel Normative Resolution No. 964, of December 14, 2021 - Provides for the cybersecurity policy to be adopted by agents in the electricity sector.

2.7 Normative Instruction IN 01/2008 GSI - Disciplines the management of information security and communications in the Federal Public Administration, direct and indirect, and makes other provisions.

2.8 Complementary Standard No. 03/IN01/DSIC/GSIPR, of June 30, 2009 - Guidelines for the Development of Information and Communications Security Policy in the Bodies and Entities of the Federal Public Administration.

2.9 ABNT NBR ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security management.

2.10 ABNT NBR ISO/IEC 27001:2013 – Information technology – Security techniques – Information Security Management Systems.

2.11 ABNT ISO GUIDE 73:2009 - Risk management.

2.12 Operational Routine - Minimum cyber security controls for the Regulated Cyber Environment (ONS RO-CB.BR.01).

2.13 Code of Ethics and Integrity.

2.14 Personal Data Protection and Privacy Policy of Eletrobras Companies.

2.15 Risk Management Policy of Eletrobras Companies.

2.16 Information Classification Regulation of Eletrobras Companies.

3 Values

3.1 Ensuring availability, so that information is accessible and usable when needed.

3.2 Ensuring the integrity of information so that it is not modified or destroyed in an unauthorized or accidental manner.

3.3 Ensuring confidentiality of information, so that it is available or disclosed only to the authorized and accredited individual, system, body or entity.

3.4 Guarantee authenticity of authorship and origin of information so that they are always identifiable.

4 Guidelines

4.1 Management of the "information" asset

4.1.1 All information used by Eletrobras companies is an asset that has value and must be properly managed throughout its life cycle, so that it is available for authorized access, protected against undue manipulation, with treatment adequate to its classification and capable of being traced.

4.2 Ownership and use of information

4.2.1 Eletrobras companies are the owners and holders of the exclusive right to use the information generated, stored, processed or transmitted in the conventional or technology environment.

4.3 Classification of Information

4.3.1 The information used in Eletrobras companies must be classified based on methodologies and criteria defined in the Eletrobras Companies Information Classification Regulation, considering the processes and activities in which they are inserted, so as to ensure that they receive an adequate level of protection, according to the value, legal requirements and criticality for Eletrobras companies.

4.4 Use of information and of corporative and operative technology resources

4.4.1 The information manager must determine the authorization of access, including those related to the business management system, taking into account the classification of the information, in compliance with the strategic objectives of Eletrobras companies.

4.4.2 Access to information should be authorized only for those employees and systems that require it in order to carry out professional activities.

4.4.3 Each employee should access only the information or systems previously authorized. Any unauthorized attempt to access information by means of corporate and operational technology resources must be investigated and may be considered disciplinary misconduct.

4.4.4 The credential *(login* and password) granted to an employee is for individual use, non-transferable and of exclusive knowledge.

4.4.4.1 In assets that do not have features of access individualization, the management of credentials is the responsibility of the information manager of their respective area, who must determine the authorization and form of access.

4.4.5 The corporate and operational technology resources provided by Eletrobras companies, including e-mail, ought to be primarily used for professional purposes. Thus, any and all use must not violate the relevant laws and regulations, as well as the Code of Conduct Ethics and Integrity.

4.4.6 To ensure compliance with this policy, the use of corporate and operational technology resources must be recorded and monitored by Eletrobras companies, as the employee must not have an expectation of privacy in this use.

4.5 Protection of Information

4.5.1 Information security should be achieved by implementing a set of appropriate controls, including policies, processes, procedures, organizational structures and technology resources.

4.5.2 Eletrobras guides, through its Code of Ethical Conduct and Integrity, that employees must "preserve the integrity of documents, records, registrations and information systems of Eletrobras companies, in all means used by the company, both physical and electronic".

4.5.3 The information manager must provide protection and control of physical and logical access to the information assets of their respective area, compatible with their classification level.

4.5.4 Any incident affecting information security must be recorded as instructed by the Regulation for the Handling of Information Security Incidents of Eletrobras Companies.

4.5.5 Information security risks should be identified, quantified and prioritized in order for adequate protection measures to be adopted.

4.5.6 The areas responsible for cybersecurity should keep up-to-date records of cybersecurity indicators, as well as the proper maintenance of the technology environment, assets, configurations and security solutions in use in the company.

4.5.7 The areas responsible for cybersecurity must monitor the vulnerabilities of their assets, in compliance with the Vulnerability Management Regulation of Eletrobras Companies.

4.5.8 The areas responsible for cyber security must inform the areas responsible for information security, in Eletrobras companies, of any data that is necessary to draft reports to the market or to the management of Eletrobras companies.

4.6 Confidentiality of Information

4.6.1 Employees of Eletrobras companies must not disclose or make use of information owned by Eletrobras companies, whether for their own benefit or that of third parties, regardless of the type of media or support used. Failure to comply with this guideline should be investigated and may be considered disciplinary misconduct.

4.7 Continuity of use of information

4.7.1 Corporate and operational technology resources used in the management, operational and support activities of Eletrobras companies, which are identified as critical to the

business, must be protected against situations of unavailability and must have defined continuity plans.

4.7.2 Eletrobras companies must define, implement and periodically test measures of prevention and recovery for disaster and contingency situations, which must include the employees and the necessary technology and infrastructure resources.

4.8 Formal relationships with third parties

4.8.1 All formal relationships with third parties (contracts, agreements, shareholders' agreements, management agreements, formation of consortiums, among others), in which there is the sharing of information from Eletrobras companies or the granting of any type of access to corporate and operational technology resources, must be preceded by confidentiality terms and contain clauses that specifically address privacy and information security.

4.9 Timeliness of information

4.9.1 Eletrobras companies must ensure that any information with evidentiary value for the purposes of audits, compliance and legal, is preserved within the form and for the deadlines required, by the legislation in force or in accordance with specific regulations.

4.10 Training

4.10.1 Eletrobras companies must include the topic of information security in their training programs.

4.11 Processing of personal data

4.11.1 Eletrobras companies must ensure the proper processing of personal data, in strict compliance with the terms of the General Data Protection Law (LGPD), appointing and ensuring the full exercise of a personal data processing officer; and establishing a channel for civil society assistance and interaction with the National Data Protection Authority (ANPD), as well as formal processes for handling incidents with personal data privacy.

4.12 Violations and penalties

4.12.1 Failure to comply with any item of this security policy must be investigated and may be considered a disciplinary offense, according to the Code of Conduct Ethics and Integrity.

5 RESPONSIBILITIES

5.1 **Eletrobras Board of Directors (CA)** - approving this policy and deliberating on the strategic information security guidelines in order to guide the implementation process in Eletrobras companies.

5.2 **Eletrobras' Executive Board of Directors (DEE)** - approving this policy and, where applicable, the derived normative documents that enable its implementation.

5.3 **Executive Boards in Eletrobras companies** - approving, when applicable, the derived normative documents that allow the implementation of this policy.

5.4 **Area responsible for the information security of Eletrobras *holding*** - drafting policies and regulations that standardize information security actions in Eletrobras companies and coordinate the Information Security Committee of Eletrobras Companies (CESIE).

5.5 **Eletrobras Information Security Committee (CESIE)** - maintaining the guidelines of this policy and monitoring the actions necessary for its fulfillment; maintaining the normative documents originated from this policy, defining and monitoring the information security framework, carrying out the annual information security planning and promoting the information security culture through training and awareness campaigns in the Eletrobras holding.

5.6 **Eletrobras Companies Operational Technology Committee (CTOEE)** - maintaining the guidelines of this policy within the scope of OT, monitoring the actions necessary for its fulfillment and maintaining the normative documents originated from this policy.

5.7 **Information Technology, Automation and Telecommunication Committee of the Eletrobras System (Cotise)** - maintaining the Integrated Information Technology, Automation and Telecommunication Policy of the Eletrobras Companies, approving its specific guidelines, guiding and monitoring the establishment and observance of processes, controls, models, standards and tools necessary for its implementation and analyzing the specific issues presented by the representatives of the companies for subsequent application in the Eletrobras companies.

5.8 **Areas responsible for information security in Eletrobras companies** - managing, in their respective company, the processes and planning of actions to implement this policy; promote training and awareness campaigns on information security; coordinate the handling of information security incidents; support the management of information security risks, defining appropriate controls in conjunction with the risk-owning areas; coordinating the implementation and maintenance of the business continuity plan in relation to the availability of information; providing support to the first line of defense; managing the process of privacy management and protection of personal data; and supporting and participating in the carrying out of the actions established by the Information Security Committee of Eletrobras Companies (CESIE).

5.9 **Areas responsible for cyber security in Eletrobras companies** - meeting the demands of the area responsible for information security of the respective company; managing cyber indicators; communicating, recording and handling cyber incidents; aligning the planning of cyber projects and initiatives with the area responsible for information security and responding to requests from the coordinator of the Information Security Incident Response and Treatment Group (GRSI); planning the cyber security of the environment in which they operate, defining the technological configurations necessary to achieve information security.

5.10 **Area managers** - ensuring the information produced by their team, carrying out its proper classification and authorization of access and contingency, as well as the mapping, implementation and operationalization of its controls, enforcing the guidelines of this policy.

5.11 **Areas responsible for the physical security** of Eletrobras companies - preventing and protecting facilities and information assets against unauthorized physical access, damage or compromise of information; regularly assessing the environment; and forwarding to the area responsible for the company's information security a report on the vulnerabilities found in physical security measures.

5.12 **Employees** - complying with this policy and other related regulatory instruments, through the use of corporate and operational information in a responsible, professional, ethical and legal manner, respecting the rights and permissions of use granted by Eletrobras companies.

6 Concepts

6.1 **Conventional environment** – composed of information assets (such as photos, microfilms, printed documents, physical projects, non-digital records in general) that are not part of the technology environment.

6.2 **Technology environment** - composed of means of storage, transmission and processing of information, as well as the equipment and systems used for such, which employ electronic or digital technologies.

6.3 **Area** - formal organizational unit, which possesses certain duties and responsibilities (directorate, advisory, superintendence, department, division).

6.3.1 **Area responsible for cybersecurity** - one or more areas formally responsible for cybersecurity in IT, OT or ET.

6.3.2 **Area responsible for information security** - area formally responsible for information security.

6.4 ***Risk* owner** - organizational unit that has authority and responsibility over risk management.

6.5 **Asset -** any resource that has value for Eletrobras companies.

6.5.1 **Information assets** - data, information and its means of storage, transmission and processing, the equipment and systems used for this purpose, the places where these means are located, as well as the human resources that have access to them.

6.6 **Authenticity** - the property by which it is ensured that information has been produced, dispatched, modified or destroyed by a particular individual, equipment, system, body or entity.

6.7 **Life Cycle of Information** - comprises the use of information, from the time it is generated, labeled, handled, stored, classified and transmitted, until its destruction.

6.8 **Classification of Information** - the process of identifying and defining appropriate levels and criteria for protecting information, with the aim of ensuring its confidentiality, integrity and availability.

6.9 **Employee** - directors, advisors, employees, members of statutory committees, service providers, interns and non-permanent service providers who work at Eletrobras companies.

6.10 **Confidentiality** - property that ensures that information is accessed only by information assets authorized by the information manager.

6.11 **Criticality** - categorization of the asset according to the level of impact of the risks associated with the business.

6.12 **Availability** - property that ensures access to information and associated resources, and to authorized information assets, when necessary.

6.13 **Area manager** - the formal head of the organizational unit.

6.14 **Information manager** - holders of areas that perform managerial activities and holders of executive bodies of senior management, according to specific norm.

6.15 **Information Security Incident Response and Handling Group (GRSI)** - group defined in the Information Security Incident Handling Regulation of Eletrobras Companies.

6.16 **Information security incident** - any confirmed or suspected adverse event affecting the protection of information systems that compromises or has the potential to compromise the availability, integrity, confidentiality, authenticity, legality and/or privacy of information.

6.17 **Information** - data, whether processed or not, that can be used for the production and transmission of knowledge, contained in any medium, support or format.

6.18 **Line of defense** - a concept that assists in structuring and clearly defining roles and responsibilities, so that action becomes integrated. Divided into three lines of defense:

1st line: responsible for implementing and operationalizing controls to mitigate information security risks (area responsible for cyber security);

2nd line: responsible for defining the guidelines and monitoring compliance by the first line (area responsible for information security);

3rd line: carries out independent assessments that permeate the full risk management cycle (internal audit).

6.19 **Privacy** - ownership of private information that can only be accessed by third parties with the prior knowledge and authorization of the personnel it concerns.

6.20 **Resource of corporate technology** - any information asset, except for human resources, in the conventional or technology environment of Eletrobras companies, belonging to Information, Automation and Telecommunication Technology (TIC).

6.21 **Operative technology resource** - the entire real-time and historical computing and telecommunications infrastructure that serves the control room and other concerned areas and is protected by the operative firewalls. (REG-TO)

6.22 **Restriction of Access** - restriction of the interaction between information assets, thus preventing physical access, logical access or information flow between information assets (such as restricting access between people and files, between services, between people).

6.23 **Risk** - combination of the probability of an event and its consequences, generating uncertainties in the company's objectives that can cause damage, loss of information, financial loss, stoppage of a service, undue dissemination, damage to reputation, among others.

6.24 **Information security risk** - potential associated with the exploitation of one or more vulnerabilities of one or more information assets by one or more threats.

6.25 **Cybersecurity** - actions on people, technologies and processes, with the aim of enabling information assets in technology environments to be able to withstand incidents that may compromise the availability, integrity, confidentiality and authenticity of data stored, processed or transmitted and the services that these systems offer or make accessible.

6.26 **Information security** - actions that aim to enable and ensure the availability, integrity, confidentiality and authenticity of information, conventional and technology environments, through methods that aim to integrate risk management, business continuity management, incident handling, information handling, compliance, accreditation, cyber security, physical security, logical security and organizational security into strategic, operational and tactical institutional processes.

6.27 **Physical security** – physical measures designed to prevent, detect and respond to unauthorized access to people, goods, valuables, equipment, and facilities related to assets.

6.28 **Operational Technology (TO)** - set of automation systems and operational communication networks necessary for management of assets, monitoring, and control of industrial operations, applied in operation centers, substations and plants, and their processes and devices; *stand-alone* monitoring and control equipment is included in this list.

6.29 **Organizational unit** - a component of the company's organizational structure that is subordinated, directly or indirectly, to a senior executive body or collegiate management body.

7 General Provisions

7.1 The guidelines established herein should guide the performance, especially that of the areas responsible for information technology, operational technology and the information security of Eletrobras companies, contributing to a single and integrated vision.

7.2 Eletrobras companies must adapt their normative documents and the controls that are necessary in conformity with the provisions of this policy. The maximum period for adequacy is 90 days from the approval by the Eletrobras Board of Directors (CA).

7.3 This policy can be deployed in regulations that are unified and valid for all Eletrobras companies, and also in specific internal normative documents in each Eletrobras company, always aligned with the values and guidelines established herein.

7.3.1 This document should be read, considered and applied along with other applicable and relevant standards, rules and procedures adopted by Eletrobras companies, including its annexes.

7.4 Eletrobras companies must ensure that this policy and its complementary normative documents are widely disseminated to their employees, aiming at its application by all those who have relationships to the organization and who are impacted, be it directly or indirectly.

7.5 This policy and other regulatory instruments subordinated to it, with the exception of the internal rules governing the reviews of normative documents of Eletrobras companies, must be updated within a maximum period of 3 years or whenever necessary, with the intent of ensuring that the technical and legal safety requirements implemented are being complied with, updated and in accordance with current legislation and aligned with the guidelines that lead the development of our business, present in our strategic planning.