NPC **0301 INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY**

INFORMATION TECHNOLOGY

Version 15 dated 10/15/2025

1. INTRODUCTION

Copel's technological capacity does not constitute an end in itself. It is in service of the corporate strategy and therefore requires conditions that transcend the simple application of technological resources.

1.1 - SCOPE

The Information Technology and Cybersecurity Policy establishes the principles and guidelines that guide the organization of people, processes, data and tools, with the aim of generating sustainable value for the business through integrated, safe, efficient action that is aligned with good management, innovation and compliance practices.

1.2 - CONCEPTS

The terms used in this policy are conceptualized and organized in the Glossary of Concepts which can be accessed on the Copel Sustainability Portal or on the Investor Relations website

1.3 - PURPOSE

To establish the principles and guidelines that guide the strategic management of Information Technology, Information Security and Cybersecurity, Data Governance and applied Artificial Intelligence (AI), ensuring the efficient and responsible use of the Company's technological assets.

Promote the creation of business value through digital transformation, effective risk management, protection of corporate information and other digital assets, and fostering technological innovation. It also seeks to ensure that investments and initiatives in technology are aligned with Strategic Planning, in compliance with best practices in governance, security, data privacy and operational resilience.

This policy applies to Companhia Paranaense de Energia - Copel (Holding), its wholly-owned subsidiaries - SIs (direct and indirect) and subsidiaries (direct and indirect), respecting its corporate processes. It is also applicable, as a recommendation, to joint subsidiaries, affiliated companies and other corporate interests, respecting their corporate processes.

1.4 - PRINCIPLES

a) **Confidentiality**: ensure that all access to information is made available only to the entities or persons duly authorized by the owner of the information.
b) **Integrity:** ensure that information is accurate, complete and protected from undue change during its lifecycle with respect to confidentiality, availability and traceability characteristics.
c) **Availability:** ensure that all information is available for use whenever authorized entities or persons require it.
d) **Traceability:** ensure the monitoring of operations in the Company's processes, according to criticality mapping, aiming to identify any type of change in information.
e) **Minimum privileges:** ensure that people, information systems and processes access only the information necessary to perform their activities.
f) **Minimal exposure:** ensure that information is kept protected, and exposed only when necessary.
g) **Duty of diligence:** all Company professionals (administrators, employees, interns, apprentices and third parties), are co-responsible for preserving and complying with Copel's information security and cybersecurity policies, performing all access and use of information in a responsible and regular manner.
h) **Compliance:** ensure that the Company's processes are in accordance with internal and external regulations, strictly following protocols required as a result of activities performed.
i) **Authenticity:** ensuring integrity of information from its legitimate source to end use.
j) **Non-repudiation and responsibility:** ensure that the source of any action in the system can be verified and

associated with a person.

k) **Data Governance:** ensure that all data is treated as assets, with governance aimed at quality, security and proper use throughout the organization.

l) **Ethics:** ensure the ethical and safe use of Artificial Intelligence (AI) and other technological assets.

2. GUIDELINES

2.1 - Information Technology resources under the responsibility of the Company must be used in an optimized, safe, ethical and sustainable manner, encompassing infrastructure, systems, data, people and services. Its use must be aligned with Strategic Planning and restricted to corporate interests, and any use for one's own self-benefit or that of third parties is prohibited, as provided for in the Company's Code of Conduct.

2.2 - All Copel collaborators must protect the company's digital assets according to their criticality and relevance to the business, adopting safe and responsible practices in the use of and access to information.

2.3 - All decisions regarding the acquisition, use or discontinuation of technological resources must consider a long-term view with criteria for performance, security, privacy, scalability, product and project portfolio, cost-benefit, environmental impact, sustainability and adherence to Copel's current corporate policies.

2.4 - Establish and maintain up-to-date IT processes based on best-in-class methodologies, clearly defining operational roles, responsibilities and flows, promoting greater efficiency, transparency and predictability in deliveries and contributing to the reduction of operational risks, better use of resources and increased confidence of the business areas in IT as a strategic partner.

2.5 - Manage IT assets to satisfactorily meet Copel services, providing resources and maintaining up-to-date asset and accounting management and control.

2.6 - Ensure the support and continuity of knowledge through its corporate systems and databases, in order to register, organize, preserve and facilitate access to knowledge generated in the company, ensuring its availability to support Copel's strategic business.

2.7 - Establish principles and practices that integrate *Environmental, Social and Governance* - ESG values into Information Technology activities, promoting responsible innovation, digital ethics, positive impact on society and value to business.

2.8 - Ensure the confidentiality, integrity and availability of information, systems and services, implementing appropriate technical and organizational controls according to the level of risk.

2.9 - Adopt a maturity model in Cybersecurity, aiming at defense, risk mitigation, strengthening organizational resilience and increasing the trust of customers, partners and regulators.

2.10 - Ensure traceability of changes and accesses to critical information during application development or acquisition, in compliance with security, audit, data privacy and corporate governance requirements.

2.11 - Manage cyber risks on an ongoing basis, identifying, analyzing and addressing risks related to digital threats, technology failures, improper access, data leakage and operational interruptions, with a focus on proactive mitigation.

2.12 - Develop an organizational environment that enables Copel to identify and manage the risks associated with information and cybersecurity, data governance and the use of Artificial Intelligence (AI) with respect to systems, processes, people, assets, data and resources.

2.13 - Develop the culture of information security and cybersecurity through the awareness of administrators, employees, interns, apprentices and third parties and the provision of means for detecting and communicating risks to the information security area.

2.14 - Establish and implement an Information Security and Cybersecurity Incident Response Plan, including event

monitoring, threat identification and rapid incident response, with post-incident registration, communication, containment and analysis.

2.15 - Perform periodic management and review of identities and accesses to Copel computing resources, ensuring the definition of minimum privileges and traceability of accesses performed.

2.16 - Develop and implement plans of resilience in order to restore any resources or services that have been harmed due to an information security and cybersecurity incident.

2.17 - Revoke collaborator access in the event of termination, change of function or department, termination of contract, prolonged inactivity or information security risk.

2.18 - Implement an Information Security and Cybersecurity Program to monitor corrective and/or preventive activities in the processes under its responsibility.

2.19 - Establish security controls as an integral part of the application development process, acquisition and life to ensure that the information processed is protected according to its classification and exposure to risk.

2.20 - Manage Information Security risks throughout the lifecycle of the relationship with suppliers and service providers, establishing the minimum applicable security requirements. These requirements will be based on periodic risk assessments, implementation of cyber protection and defense mechanisms, adherence to current security policies and controls, including the performance of training and awareness actions, and the obligation to manage and report any information security and cybersecurity incidents that may impact the Company on a timely basis.

2.21 - Continuously raise safety levels, providing continuous improvement in Copel environments and systems.

2.22 - Ensure that generative Artificial Intelligence (AI) is used in an ethical manner, strictly respecting data privacy and ensuring that critical, personal or confidential information is not exposed without authorization.

2.23 - Establish controls necessary for the use of AI in Copel environments and systems, ensuring its traceability and protecting from data manipulation and critical data leakage.

2.24 - The collaborator must use AI in environments that are controlled, secure and authorized by the Information Technology area, respecting privacy and security processes, in addition to the standards in force at Copel.

2.25 - Any person, regardless of position, function or workplace will be responsible for any breach or violation of this policy, through the management of consequences to be performed by the company in accordance with the internal and external regulations in force.

3. SPECIFIC LEGISLATION RELATED TO THE SUBJECT

The laws and regulations that directly affect Copel's Corporate Policies are organized in the Legislation Notebook of Reference, which can be accessed on the Copel Sustainability Portal or on the Investor Relations website.

It updates NPC 0301 of 05/28/2024 and incorporates the content of NPC 0302 - Information Technology Policy, of the same date.

NPC 0107 approved by the 267th Ordinary Meeting of the Board of Directors (ROCAD, *Reunião Ordinária do Conselho de Administração*), of 10/15/2025.