INFORMATION SECURITY POLICY

1. GENERAL PROVISIONS

Approved at the 10th Ordinary Meeting of the Board of Directors, held on October 19, 2023 (Version 3).

2. PURPOSE

The purpose of this Information Security Policy is to establish principles, guidelines, responsibilities, and concepts to be observed for Sanepar's Information Security within the scope of the Information Security Management System and the Integrity Program.

The purpose of this Policy is to protect the Company's data, documents, and information, to safeguard them, aiming at the smooth conduct of business through best practices, seeking economic, social, and environmental sustainability, protection against unfair competition, collusive or fraudulent practices, always aiming at the efficiency of processes and the absorption of innovations, whether said data, documents or information are stored using conventional or technological means, internal or external to the company's physical area and made available on file sharing platforms.

3. SCOPE

This policy applies to those who may have access to Sanepar's information, managers, members of Councils and Committees, employees, interns, apprentices, suppliers, contractors, service providers in general, and to all business partners, regardless of denomination or contractual relationship with which they present themselves.

Information Security Policy can be found at: http://www.sanepar.com.br and, once approved by the Board of Directors, it must be disclosed to all those who must comply with it.

4. REFERENCES

4.1 Constitution of the Federative Republic of Brazil;
4.2 Federal Law No. 12,527/2011 (Access to Information Act);
4.3 Decree 10,285/2014 (Provides for procedures to be observed by the Direct and Indirect Administration, to guarantee access to information);
4.4 Federal Law No. 13,709/2018 – General Personal Data Protection Law (LGPD);
4.5 Federal Law No. 12,965/2014 (Civil Rights Framework for Internet);
4.6 Federal Law No. 6,404/1976 (Deals with Corporations);
4.7 Federal Law No. 13,303/2016 (Provides for the legal status of state-owned companies, government-controlled companies, and their subsidiaries, within the Federal Government, States, Federal District, and Municipalities);

4.8 Law 12,846/2013 (Provides for the administrative and civil liability of legal entities for the practice of acts against the government, domestic or foreign, and other measures);
4.9 Resolution No. 55/2021 - CGE;
4.10 ISO 27,001 – Information Security Management Systems;
4.11 Personal Data Protection and Privacy Policy; and
4.12 Code of Conduct and Integrity;
4.13 Code of Conduct and Integrity for Suppliers and Business Partners of Sanepar;
4.14 CAVOUKIAN, Ann et al. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, v. 5, 2009.

This Policy must be read and interpreted together with the Bylaws, and other corporate policies, mainly the Information Protection Regulation, Sanepar's Code of Conduct and Integrity.

5. DEFINITIONS

The terms and expressions listed below, when used within the scope of Sanepar's Policy Information Security, will have the following meaning:

5.1 **Conventional Environment:** The environment in which the user directly accesses data or information, which may be arranged directly on the physical support (device) for reading, such as paper, or through sound, visual means, such as oral communication, or others through from which both data and information can be accessed directly by the receiver.

5.2 **Technology Environment:** The environment in which the user relates to data and information through physical support, using technology equipment, such as computers, tablets, and mobile phones. In this environment, the information is in physical support, in digital format.

5.3 **Data:** Elementary structure of the informational chain, which can be transformed into information. Requires context to be understood.

5.4 **Information:** The term information, for this policy and other rules relating to Information Security, must also cover the data itself which, alone or together with others, will lead to the information itself.

5.5 **Information Security:** these are the administrative, technological, and physical measures adopted to preserve the confidentiality, integrity, and availability of information considered important to the company, throughout its life cycle.

6. PRINCIPLES

The guidelines of this policy must be interpreted under the principle bias, representing guidance on how data and information can be used.

This policy should serve as a guide for drawing up other rules on matters that may affect the use and provision of data and information and, consequently, the need to observe their protection, guaranteeing the attributes of:

6.1 **Availability:** the information must be accessible for legitimate use, by those who have authorization provided by the Data Controller;
6.2 **Integrity:** the information must be correct, true, and not corrupted;
6.3 **Confidentiality:** The information must be accessed and used only by users with previously granted permission due to their function, to meet the requirements of the exercise of their professional activities in the company;
6.4 **Authenticity:** the information must come from the stated source, and must not have been subject to changes during the process; and
6.5 **Legality:** the information must meet legal requirements, always in compliance with current legislation.

7. GUIDELINES

This Information Security Policy includes general guidelines and guidelines related to security by design, as described below

7.1 General Guidelines

I. Ensure that both data and information are used to obtain their institutional purposes, ensuring business continuity.
II. The development of data governance should be encouraged, with the objective of better planning, availability, monitoring, control, and security of corporate data, enabling the company's business structure to be improved;
III. Ensure that the confidentiality level of the information is classified considering the level of confidentiality of the information, the privacy of personal data to protect personal data and the data that must be considered public, according to the classification established in specific legislation and Sanepar's Regulation for Information Protection. Information confidentiality must be maintained throughout the information use process and may have different levels throughout its life cycle;
IV. Ensure that each piece of information has an Information Manager (or Group of Information Managers);
V. Ensure that the use of information is in accordance with the need for access and confidentiality of information to achieve the company's objectives;
VI. Ensure that access to information is authorized only to users who need it to carry out their professional activities for Sanepar;

VII. Ensure that each user only accesses previously authorized information and environments, considering that information access data, consisting of user identification and authentication, in a technology environment, are individual and non-transferable;

VIII. Manage and review identities and access to Sanepar's computing resources, ensuring minimum privileges and traceability of accesses are set.

IX. Ensure that user authentication data is kept secret, considering the highest level of information classification;

X. Ensure that all Sanepar information is protected so that it is not improperly altered, accessed, and destroyed. Locations at which information resources are located must have protection and physical access control compatible with their level of criticality;

XI. Ensuring that corporate information has sufficient backup copies to maintain business continuity plans;

XII. Ensure that the infrastructure technological resources and the physical environments where Sanepar's business operational activities are carried out must be protected against unavailability situations and have business continuity plans;

XIII. Ensure that preventative and information recovery measures for disaster and contingency situations are taken continuously and include technology, human, and infrastructure resources;

XIV. Ensure that information technology resources are used solely for professional activity and within the limits necessary for their exercise;

XV. Ensure that every project considers information security as a pillar of planning, development, and review of processes and systems;

XVI. Ensuring the management of assets associated with information and information processing resources; and

XVII. Ensure and prioritize the mitigation of infrastructure resource vulnerabilities.

7.2 Security by Design

Security by Design means that technology products are built to reasonably protect against malicious activity that may successfully gain access to devices, data, and technology infrastructure. Those involved in the management, development, design, and maintenance of technology must perform a risk assessment to identify and enumerate the prevalent cyber threats to critical technologies and then include safeguards in product designs that take into account the evolving cyber threat scenario.

All projects, products, and processes to be developed for Sanepar must undergo Information Security analysis from their inception, with the aim of enabling and ensuring the fundamental pillars of security in order to ensure the

availability, integrity, confidentiality, and authenticity of the information, represented by the principles listed below:

Security by Design Principles

I. Minimize attack surfaces

It corresponds to the identification of vulnerabilities and attack vectors in the digital aspect (websites, software, servers, etc.) or physical (devices, storage, sensors, controllers, etc.) that a malicious agent could use.

Means and techniques must be developed to reduce these surfaces, such as: access control mechanisms, profile restrictions, use of approved software and components, and security protocols for remote access, among others.

II. Establish Security Standards

Assign high-security standards to technology projects. Standardization is an important factor in designing security intelligently, as it enables more efficient, reliable, and even economical solutions to be created.

Adopting stricter security standards, such as using a secure technology design framework, ensures technology assets are safer and more susceptible to continuous improvements.

III. Adopt the principle of minimum privilege

When providing access to users, only strictly necessary privileges should be granted. The idea is to receive authorization to have privileges only to perform a certain activity, relevant to the operator's duties.

It is important to pay attention to the permissions requested to access a service. Not sharing sensitive information and setting privacy management protocols are examples of actions related to this principle.

Whenever the availability of access to resources that goes beyond the need for carrying out daily activities is identified, this fact must be reported to your Manager, with the aim of removing unnecessary access.

IV. Defense in depth

It is a set of practices that focus on protecting, detecting, and reacting to intrusions. For such purpose, processes, security software, and tools are used to build a strategy against possible attacks.

Adding security layers at all levels of a technological asset, instead of just creating primary layers of validating inputs or business rules, is a good practice.

V. Security failure

Failures must not compromise security or expose critical information. Following the idea of fail-safe and fail-fast, failure, and error messages should be presented as early as possible and prevent this from occurring at crucial moments, in addition to carefully filtering the information exposed in an error log, for example.

Secure error handling is an important aspect of secure software. There are two types of errors worth highlighting:

a) The first are exceptions that occur when processing a security control.
b) The other type of security-relevant exception is in code that is not part of a security control.

It is important that these exceptions do not allow behavior that the system would not normally allow. Software developed with security must consider the existence of three possible results of a security mechanism: prohibit the operation, allow the operation, or throw an exception.

VI. Do not trust services

Third-party services and components should be considered potential threats until in-depth validation. Every outsourced service must be considered insecure as a rule, as it may contain attack vectors or even malicious purposes in itself, compromising the security of the application.

Therefore, every service must be validated and monitored according to strict security standards.

VII. Segregation of roles and responsibilities

This is an access control based on a user's role, activity, or function within a system. The use of a role profile (or RBAC – Role-Based Access Control) provides a model for managing access privileges to a company's systems and infrastructure. The role profile can group access, providing an overview of privileges and controlling access in a secure way.

VIII. Avoid security by obscurity

Security by obscurity occurs when developers code systems secretly, believing that no one will be able to find vulnerabilities in the software. The problem with this technique is the dependence on the secrecy of project implementation as the main form of providing security for the system. Generally, people who use this technique assume that not knowing about software vulnerabilities is an indication of security.

To avoid security by obscurity, we need to invest in proven systems security practices.

IX. Keep security simple

Very complex architectures can make applications much more susceptible to errors. The greater the complexity of a technological asset, the more details and security flaws may go unnoticed, that is, excessive complexity results in a much less secure application.

The existence of many tools can increase security gaps instead of closing them, as well as poorly documented procedures or lack of automation that can leave users waiting too long for access.

It is necessary to reflect on the relevance and complexity of controls, whether they add more security or bureaucracy to systems.

X. Maintenance and safe troubleshooting

Vulnerability management must be applied as a manner to identify and map vulnerabilities, as well as their risks and forms of mitigation. Additionally, adopting continuous improvement strategies are best practice for a safer technology project.

It is necessary to understand the behavior of vulnerability structurally in the technological asset and check whether there are other components that can be affected by the same vulnerability.

The lack of a process or control to perform problem corrections can cause new problems and security breaches to emerge in technological assets. A continuous vulnerability management process is seen as an ally for project and product teams, working to identify, analyze, classify, and treat vulnerabilities. This process seeks to measure progress and assess the risks to which systems are subjected, collaborating with an appropriate strategy.

8. RESPONSIBILITIES

This Policy establishes responsibilities for the Information Security Committee, Permanent Technical Committee for Information Security, Transparency Agent, Audit, Corporate Management, Regional Management, Information and User Manager listed below:

8.1 Information Security Committee

I. Issuing guidelines to the different departments of the company for developing and implementing projects, procedures, actions, instructions, and regulations to develop an Information Security Management System, supported by this policy;
II. Discuss and deliberate on content related to information security, as well as define guidelines and strategic guidance related to the topic;
III. Respond to incidents (for example: theft and robbery of corporate data and information).

8.2 Permanent Technical Committee for Information Security

I. Support in defining actions in the Information and Communication Technology environments, in line with the Information Security Committee corporate guidelines;
II. Establish appropriate technology standards and controls;

8.3 Transparency Agent

I. Support information managers in defining the level of confidentiality and the respective classification of information, which will serve as a guideline for the application of information security;
II. Ensuring compliance with the rules relating to access to information, efficiently and appropriately to the objectives of the current legislation on access to information;
III. In the exercise of their responsibilities, the Transparency Agent will have free access to all documents, data, information, and other elements considered indispensable for the fulfillment of their responsibilities, and under no pretext may any process, document or information be withheld, unless classified under any of the degrees of confidentiality provided for in the legislation on access to information.

8.4 Audit

I. Carry out an assessment audit regarding adherence to the policy in the Company's departments, contributing with recommendations for improving information security, providing feedback on processes.

8.5 Corporate Management

I. Standardize the processes related to its area of operation, observing this and other company policies, with the guidance of the Information Security Committee;
II. Raise awareness of Sanepar's Policy Information Security according to its scope;
III. Periodically promote training and guidance on information security concepts, rules and procedures, both in general corporate terms and specific to its activity;
IV. Appoint an Information Agent (or Group of Information Agents) for each group of information relating to the main processes in the department.

8.6 Regional Management

I. Raise awareness of Sanepar's Policy Information Security according to its scope;
II. Periodically promote training and guidance on information security concepts, rules and procedures, both in general corporate terms and specific to its activity.

8.7 Information Manager

I. Authorize and allow access, validation and inspection of the use of data and information, and define controls;
II. Assist the Transparency Agent in reviewing the Company's list of protected information;
III. Classify the level of confidentiality and secrecy of the information internally, according to the internal rules and the prerogatives of the process.

8.8 User

I. Be responsible for the security of the information to which they have access in any way;
II. Avoid unnecessary exposure of data and information in their possession, even if it is the object of their position or function, and care for information classified as internal regulations as in their periods;
III. Take care of the information technology resource made available by Sanepar, with the individual responsible for those resources provided to them.

9. RESPONSIBILITIES

9.1 Failure to comply with the responsibilities set forth in this Policy must be reported both to the Information Security Committee and to Governance, Risks and Compliance Management and will be treated in accordance with the provisions of Sanepar's Code of Conduct and Disciplinary Regulations, without prejudice to incidence of other norms that regulate issues of information security and labor relations.

9.2 Failure to comply with the provisions contained in this policy, and other rules relating to Information Security, may result in the application of disciplinary measures in accordance with Sanepar's Integrity Program, regardless of administrative, civil and criminal liability.

10. REVISION

This policy must be revised periodically or extraordinarily when there is a relevant fact to justify it. Reviewing the policy will require prior communication to the departments responsible for maintaining the affected standards so that they can be reviewed, maintaining coherence with the policy.

11. FINAL PROVISIONS

Doubts regarding the interpretation of this Policy can be clarified with the Information Security Committee.

This policy is effective on the date it is approved by the Board.

12. HISTORY

Information Security Policy			**Version**	2
			Management Department	DAGRC
			Confidentiality	External Audience
Version	**Date**	**Person in Charge**	**Approved by**	**Description of Change**
1	08/27/2020	Governance, Risk and Compliance Board	Board of Directors	First Issue
2	11/17/2022	Governance, Risk and Compliance Board	Board of Directors	First Review
2	10/19/2023	Governance, Risk and Compliance Board	Board of Directors	Second Review, inclusion of security by design