Raízen Policy – PLT.01

Information Security Policy

1. Objective

The purpose of the Information Security Policy ("Policy") is to establish guidelines, responsibilities, and general principles of information and cyber security, with the aim of preserving the confidentiality, integrity, availability, authenticity, and non-repudiation of Raízen S.A.'s ("Raízen" or "Company") information assets, in alignment with market best practices and in compliance with applicable regulations.

2. Guidelines

Information security encompasses five fundamental pillars, highlighted below:

• **Confidentiality:** Restrict access to information and information assets only to authorized users, processes, and devices, preventing disclosure, exposure, or misuse.

• **Availability:** Maintain information and information assets accessible to authorized users whenever required, throughout their entire lifecycle.

• **Integrity:** Preserve the integrity and completeness of information and information assets, protecting them from unauthorized alterations, deletions, or insertions resulting from failures or misuse.

• **Authenticity:** Validate the origin and ownership of information, confirming that it originates from the declared source and remains unaltered throughout the established process.

• **Irrevocability (non-repudiation):** Implement mechanisms that enable the traceability and verification of the origin, transmission, and receipt of information, preventing the denial of authorship or responsibility.

3. General Aspects

- The protection of information and corporate assets must be considered across all processes and business areas.
- Information must be handled in compliance with applicable laws, internal policies, and solely for the purposes for which it was collected.
- Raízen's information and information assets must be protected in accordance with their level of criticality and business impact, in compliance with applicable laws and internal policies, and used solely for their intended purpose
- Raízen adopts measures to ensure the secure use of technological resources, including monitoring and traceability when necessary.

- Technologies, methodologies, and corporate data must not be shared or used for personal purposes, except with explicit authorization.

4. Information Classification

- Information is classified according to its sensitivity level, business impact, and need for protection, and may be categorized as Public, Internal, Confidential, or Restricted. Each employee is responsible for the appropriate classification of the information they generate or handle.

5. Protection of Personal and Sensitive Data

- Raizen n has a Data Privacy and Protection Program aligned with the Brazilian General Data Protection Law (LGPD), incorporating structured governance, risk management, and a privacy culture across the organization.

6. Cybersecurity

- Industry best practices and solutions are adopted to protect the organization's digital assets, including user authentication, encryption, prevention of unauthorized access, malware protection, activity monitoring, network segmentation, and vulnerability management.

7. Incident and Risk Management

- The company maintains structured processes to identify, assess, and address information security risks, as well as specific procedures for responding to incidents in both IT and OT environments.

8. Training and Awareness

- Through the "Guardião" Program, Raízen promotes ongoing training and awareness initiatives on information security, engaging all levels of the organization.

9. Supplier Security

- Suppliers and partners must comply with Raízen's information security requirements, including contractual obligations and risk assessments, ensuring alignment with industry best practices.

10. Continuous Improvement

- Raízen is committed to the continuous improvement of its information security processes, controls, and guidelines, including periodic reviews of this Policy and related documents to ensure effectiveness, alignment with industry standards, technological evolution, and compliance with applicable legal and regulatory requirements.

11. Question and Reporting Channel

- Employees, partners, and third parties may report questions or potential violations of this Policy through official channels, with confidentiality and protection against retaliation ensured.