Corporate Policy

Technology and Information Security

1 OBJECTIVE

The Policy on Technology and Information Security establishes concepts and guidelines for managing FORESEA's technological environment, comprising infrastructure, systems, applications, assets and security of data manipulated in digital or physical means, by members or partners in the development of their activities, aimed at ensuring the protection of information, as well as supporting FORESEA's strategic goals.

The goals of this Policy are:

- To establish and/or guide FORESEA's members and partners on:
  - the importance of information security for preventing and reducing risks and ensuring integrity, secrecy and availability of information;
  - standards for creating, receiving, withholding and destroying data, records and information produced during the course of business activities;
  - how to act to ensure the availability, integrity, confidentiality, legality, authenticity and traceability of the information necessary for FORESEA's sustainability;
- To support FORESEA in their business purposes and comply with the legal and regulatory requirements;
- To serve as a reference for any initiative or process related to information or information processing assets;
- To define the responsibilities of information security management.

2 APPLICATION

This Policy is applicable to FORESEA, including their subsidiaries that do not have a Board of Directors, to all members, Officers and members of the Board of Directors, in any jurisdiction.

In addition, this Policy serves as a guide for the members of the board of directors appointed by FORESEA, in subsidiaries or affiliates, so that, in line with all other directors, they approve and implement a policy on information technology and security containing the principles, concepts and all other guidelines defined and explained in this policy, without neglecting, however, to promote the complements and other guidelines which are necessary for adaptation to the characteristics of their respective businesses and to the contributions of all other directors.

3 ACRONYMS AND DEFINITIONS

Action Program (PA): A document explaining the responsibilities of members in a given period, whose focus is the expected results of the work of each one and not the tasks that must be performed. It also contains the delegation they receive, and the commitments they take on.

Availability: guarantee that the information will be accessible to people, automated processes, agencies or entities at the time it is required. Therefore, availability pertains to the continued rendering of a service, with smooth provision of information.

Authenticity: is the property that the information was produced, issued, modified or destroyed by a specific individual or by a specific system, agency or entity.

Backup and data management: process aimed at ensuring integrity, authenticity and legality of the information registered by users at FORESEA.

CA-FORESEA: Board of Directors of FORESEA. Executive collegiate, deliberative body, responsible for approving the strategic direction and monitoring the company's performance, deliberating on other matters within its competence and exercising the control functions that are relevant to them.

COMEX: Executive Committee.

Confidentiality: implies preventing unauthorized, inadvertent or intentional access, ensuring that only duly authorized and accredited people, systems, agencies or entities have access to the information.

Firewalls: computer network device, in the form of a program or physical equipment, which aims to apply a security policy to a specific point of the network, generally associated with TCP/IP networks.

Information security incidents: an information security incident is one or a series of unwanted or unexpected events with a significant probability of jeopardizing business operations and threatening information security (ISO/IEC 27000 2.36).

Information: property of FORESEA, consists of all Information produced, conveyed or stored within the scope of the business, which may be of an engineering, commercial, financial, administrative, strategic, marketing, legal or of any other nature, as well as all information obtained by contract, association, acquisition or consolidation, as well as those relating to customers or partners, among others (protected or not by confidentiality), regardless of form (oral and written) and support (physical or digital).

Information Owner: member or partner in charge of preparing the information or recipient of outside information.

Information Security: group of Information protection measures adopted by FORESEA, so that they are known only by those who must know them for the development of their PAs, preventing its improper, inappropriate or illegal use.

Information Technology Infrastructure: assets that encompass all Information Technology resources, proprietary or third-party, such as, but not limited to servers, data centers, desktops, notebooks, tablets, smartphones, data cards, cell phones, IP phones, printers, Internet links, telephone lines, IoT devices, among other resources which may eventually be used in the future due to technological innovation.

Integrity of information: is related to its reliability. Ensuring the integrity of information, therefore, means ensuring the information was not changed or destroyed in an unauthorized manner, either inadvertently or intentionally.

IT: Information Technology.

Legality: ensures the use of the information follows the applicable laws of countries, regulations, licenses, and contracts.

LGPD: General Law for the Protection of Personal Data, Law No. 13,709/2018, is the Brazilian law that regulates the activities of processing personal data, including in digital media, by individuals or legal entities governed by public or private law, aimed at protecting the fundamental rights of freedom and privacy and the free development of the personality of individuals.

Partner: service providers, business partners and all those who are not classified as members and who interact with FORESEA's information.

Person in charge of managing Information: person in charge of managing FORESEA's data, also acting as Data Protection Officer (DPO), in compliance with the LGPD.

Traceability: is the property of setting up systems and access to information enabling the tracking of physical and logical activities.

4 DESCRIPTION

4.1 Information Security Workgroup

The Information Security Workgroup is permanent and manages Information Security within the scope of FORESEA. It is multidisciplinary in nature and comprises the Person in Charge of Information Technology, the Person in Charge of Information Management, a representative of the People team, a representative of the Legal team and a representative of the Compliance team.

4.2 Information Classification

The Information must be classified by their owner in accordance with the rules and standards defined in a regulatory document prepared by the Information Security Workgroup, the information being identified according to the level of secrecy, its importance and criticality for the development of the business and in line with applicable legislation.

4.3 Information Access Control

It is up to the Person in Charge of Information Technology at FORESEA to provide and manage the systems for managing identities and controls of logical access to systems and the network to minimize risks of unauthorized access to information.

The owner of the information asset is usually the person who operates the *asset* and who ensures that the *information* related to such *asset* is protected. It is up to the owner of the information asset to approve all requests for access, revocation and monitoring of information, Information Technology Infrastructure and Information Systems for members and partners, depending on the performance needs of their Action Programs.

Access to information, Information Technology Infrastructure and Information Systems must be conducted by a personal, non-transferable user (login), in order to ensure the traceability of actions.

Access to FORESEA's systems and corporate network from the corporate environment or from the external environment via remote access is only granted after approval by the immediate leader of the member (or manager of the partner's agreement) and/or by the owner of the information asset. All privileges are strictly in line with the performance of the user's activities for as long as necessary and are reviewed at least every 12 months.

Passwords are personal and non-transferable, and it is up to the member to keep them safe and secret. It is up to the person in charge of Information Technology to define the mandatory parameters to be used for managing passwords, in order to ensure the confidentiality, integrity, authenticity and legality of information.

4.4 Use of the Information Technology Infrastructure and Information Systems

The Information Technology Infrastructure and Information Systems provided to members, service providers and authorized business partners are used only to serve FORESEA's business interests.

The Internet access provided is a work tool and must be used to meet the company's business purposes. FORESEA may block access to websites and applications they deem incompatible with the purpose of the business, suspicious or with a questionable reputation.

All corporate equipment, such as desktops, notebooks and mobile devices which are under the custody of members and partners must have implemented the minimum security requirements defined by the Person in Charge of Technology at FORESEA for internal and remote access to the corporate network.

Personal mobile equipment and devices for accessing FORESEA's corporate systems may be used provided the requirements specified by the Information Technology Area are met.

Only software ratified by the Information Technology team must be installed in FORESEA's Information Technology Infrastructure, the installation being the sole responsibility of the IT team. It is also up to the IT team to monitor the use of software on corporate equipment, aiming at removing any and all non-ratified or unlicensed software.

It is forbidden to use FORESEA's Information Technology Infrastructure and Information Systems to express personal opinions of any nature, distribute or access copyrighted material, advertisements, jokes, pornographic content, solidarity chains, electronic games or content breaching rights of FORESEA or third parties.

Access and use of corporate email with pornographic content, pedophilia, supporting illegal activities, despising, belittling or inciting prejudice against any classes, promoting public discussion without consent concerning FORESEA's activities or any other content that does not adhere to FORESEA's Code of Conduct are subject to disciplinary action.

The Person in Charge of Information Technology, together with the Person in Charge of Information Management at FORESEA, defines the rules for routine creation of backups of systems or information assets, in order to ensure the withholding of information for the established legal periods and the continuity of business activities.

Managing FORESEA's email services and digital certificates is the responsibility of the Person in Charge of Information Technology.

The entire Information Technology Infrastructure, Information Systems, computers and mobile devices are subject to monitoring by FORESEA, the members being aware that they may be audited at any time in their use and held accountable for their actions.

4.5 Protection of the Information Technology Infrastructure

It is the responsibility of the Person in Charge of Information Technology at FORESEA to:

- Ensure that good information security practices are applied in the purchase of equipment and systems, in the setting up of the environment, preventive tests, periodic reviews and in the training, both of the Technology team and of FORESEA's members, in order to prevent data loss and external attacks on the corporate environment;
- Prevent any unauthorized physical and logical access, risks of damage or interferences in information processing resources;
- Define the processes and means of monitoring that ensure that only authorized agents access FORESEA's environments;
- Define and manage firewalls, essential equipment to ensure logical access to corporate environment.
- Provide physical barriers and controlled access, using appropriate security systems and mechanisms, to locations dedicated to the installation of FORESEA's critical Information Technology equipment, including Data Centers and a Data Processing Center.

4.6 Security with Suppliers and Business Partners

Information security requirements to prevent and/or mitigate risks associated with supplier and business partner access to FORESEA's assets must be formally agreed upon and documented.

The member in charge of the agreement addresses the information security risks in each contracting, by consulting the Person in Charge of Information Technology at FORESEA regarding security risks and controls to be used for prevention and/or mitigation, whenever required.

4.7 Acquisition, Development and Maintenance of Systems

Information security requirements must be part of the entire lifecycle of information systems from acquisition, development of new systems and/or improvement of existing ones.
Any activity involving the lifecycle of information systems must be assessed, ratified and approved by the Person in Charge of Information Technology at FORESEA.

4.8 Early Termination of Employment Agreements

In cases of early termination of employment agreements, members shall return to the Information Technology team all Information Technology devices (cell phone, notebook, tablet, etc.) in their possession. Before enforcing the early termination of the member's agreement, the People team ensures with the Information Technology team that the equipment has been returned.

4.9 IT Service Continuity Plan

It is up to the Person in Charge of Information Technology at FORESEA to implement measures so that critical IT services have a continuity plan to mitigate unavailability and data loss in the event of an incident, ensuring the continuity of actions to fulfill the company's commitments.

4.10 General provisions

If there is any doubt about the content of the Policy on Information Security and Technology, a member cannot omit and must seek clarification through their direct leader or, if necessary, through the FORESEA Information Technology team.
Members, interns and temporary employees who violate or attempt to violate the guidelines described in this Policy and in its developments are subject to the enforcement of disciplinary action.
In case of Third Parties who are contrary to the provisions contained in this Policy and in its developments, appropriate action will be taken, which may also result in the enforcement of contractual penalties, agreement termination and legal execution of compensations for losses incurred by FORESEA.

4.11 Awareness & Certification

All FORESEA members and all other audiences covered by this document must be aware of this Policy on Information Technology & Security within a maximum of 90 days after the date of its approval.

5 RESPONSIBILITIES

5.1 Members

- Must be familiar with and act in accordance with this policy when creating, receiving, managing, storing and disposing of FORESEA's data, records and information;
- Preserve the integrity and keep confidential the data and information they use, and also safeguard and protect their respective information processing resources;
- Keep the passwords for accessing FORESEA's Information systems and resources confidential;
- They must not share, in any form, confidential data and information with others who do not have the proper clearance;
- They must not breach the relevant legislation applied to each country where FORESEA operates;
- Protect, at the physical and logical levels, and look after the assets that store or process FORESEA's data;
- They must immediately report to their leader and/or through the Ethics Line Channel, any knowledge of irregularity or deviation (security incident) of this Policy.

5.2 Leaders

- They must communicate and encourage their subordinates about the importance of protecting FORESEA's data and information and ensure compliance with the guidelines and rules provided for herein;
- Whenever questioned, they must report to the Person in Charge of Information Technology at FORESEA about information security in their businesses, areas and concerning their subordinates.

5.3 Information Security Workgroup

- Deals with issues related to FORESEA's Information Security, ensuring alignment and compliance with this Policy, in addition to analyzing any breaches of this Policy perpetrated by Members and/or partners.

5.4 Person in Charge of Information Technology

- Develops and keeps the Policy on Information Technology and Security up to date, as well as its consequences;
- Leads the Information Security Workgroup and advises the President, Vice Presidents and all other FORESEA leaders;
- Promote actions to raise awareness and training on this Policy and its consequences;

- Reports on FORESEA's Technology and Information Security performance to COMEX and to CA-FORESEA through a specific advisory committee.

5.5 Person in Charge of Managing Information

- Develops and keeps the guidelines and all other developments of this policy updated, aiming at guiding the action of the Person in Charge of Information Technology, leaders and all other members.
- Responds as the person in charge of processing FORESEA's personal data, assuming as such the responsibilities established in the General Data Protection Law.

6 REFERENCE DOCUMENTS

- ABNT ISO/IEC 27001:2013.
- ABNT ISO/IEC 27002:2013.
- Law No. 13,709/2018 – General Data Protection Law (LGPD).
- Code of Conduct of FORESEA.

7 REFERENCE PROCESSES MAPS

NA

8 ANNEXES

NA