INSTITUTIONAL DOCUMENT

INFORMATION SECURITY

2nd edition

INTRODUCTION

Information Security (IS) plays an increasingly important role for the companies of the Senior Group. Hence the need to protect information and information assets regarding risks and threats that arise in this area.

The Senior Group, aware of the relevance of this matter, prepared this document, reinforcing the transparency and patronage of the theme, with the aim of serving as a guide for customers and the industry.

Carlenio Castelo Branco

President

INDEX

2.4 Cookie Policy

2.5 Contact of Holders

2.6 Mapping of Personal Data and Processing Activities Record (ROPA)

2.7 Personal Data Impact Analysis (AIPD)

3. COMPLIANCE AND CERTIFICATIONS

a. ISO 27001

b. SOC 1 Type II

4. FAQ

1. INFORMATION SECURITY

In this item, concepts related to the Information Security Policy will be presented, as well as issues that demonstrate the importance of its preparation, implementation and disclosure.

1.1 WHAT DOES INFORMATION SECURITY AIM AT?

Information Security plays a strategic role in the Senior Group and aims to guarantee the integrity, confidentiality, authenticity and availability of the information processed by the institution. The integrity, confidentiality, authenticity and availability of information will be addressed in the following items.

1.1.1 What is information integrity?

It consists of the reliability of information. Signals compliance of stored data with respect to authorized insertions, alterations, and processing carried out. It also signals the conformity of the data transmitted by the sender with those received by the recipient. The maintenance of integrity considers the guarantee of non-violation of the data with the intention of alteration, recording, or deletion, whether accidental or deliberate.

1.1.2 What is information availability?

It consists in ensuring that the information is accessible to authorized persons and processes, at any required time, during a previously agreed period. Maintaining the availability of information means ensuring the continuous provision of the service, without interruptions in the provision of information to those entitled to it.

1.1.3 What is information confidentiality?

It consists of ensuring that only authorized persons have access to information stored or transmitted through communication networks. Maintaining confidentiality considers ensuring that people do not become aware of information, accidentally or on purpose, without having authorization for such a procedure.

1.1.4 What is information authenticity?

It consists of guaranteeing the veracity of the source of information. Through authentication, it is possible to confirm the identity of the person or entity providing the information.

1.2 INFORMATION SECURITY POLICY TOPICS

The Information Security Policy is a formal document, approved by Senior Group's board of directors, which aims to implement the best information security practices, with the purpose of assigning responsibility, defining rights, duties, expectations of access and use, penalty and promote an organizational educational culture of security and privacy of the Senior Group's information, customers, suppliers and partners.

1.3 INFORMATION SECURITY POLICY TOPICS

Senior Group's Information Security Policy is a complete document organized by topics. Respecting the Information Classification Policy, this document is restricted to Senior Group employees and third parties. A brief description of each control is described below:

1.3.1 Responsibilities

This topic describes all the general roles and responsibilities of the institution, its employees and third parties, including senior management, on the topic of Information Security in the Senior Group.

1.3.2 Password Policy

This topic describes the minimum requirements acceptable by the business to configure access passwords to Senior Group's technology environments. Internal controls are implemented to require passwords to be configured with a

minimum number of characters, blocking due to a number of attempts and frequency of change, as well as blocking the reuse of previous passwords.

1.3.3 Access Control Policy

This topic describes general guidelines for accessing information assets and systems. Accesses are segregated between logical access and physical access.

1.3.3.1 Logical Access:

The logical access policy defines guidelines such as:

• Access Profiles;

• Concession, Revocation, Revision and Cancellation of accesses;

• Third Party Access;

• Remote access;

• Multiple Factor Authentication (MFA)

1.3.3.2 Physical Access:

The physical access policy defines guidelines such as:

• Turnstiles;

• Gates;

• Security cameras;

• Surveillance professionals;

• Generators and UPS;

• Lightning rod;

1.3.4 Policy for Use of Mobile Devices and Assets

This topic describes guidelines for using corporate assets in a safe, professional, ethical, and legal manner, as well as requirements for protecting information during asset transportation.

1.3.5 Information Classification Policy

This topic describes guidelines for classifying information in the handling, labeling, transfer, and storage of information assets. The internal document provides all the guidelines used to classify information, as well as its categories.

1.3.6 Clear Desk and Clear Screen Policy

This topic describes guidelines on how to handle, store and protect information when using workstations provided by the business, to prevent unauthorized people from accessing restricted information, maintaining the principle of confidentiality. Internal controls are in place to ensure the automatic locking of workstations, preventing inappropriate exposure of data.

1.3.7 Information Transfer Policy

This topic describes guidelines to ensure that information regarding the Senior Group and its customers, third parties and suppliers is transmitted in a secure manner. Internal controls are implemented to ensure security during data transfer, inside and outside the company's infrastructure.

1.3.8 Remote Work Policy

This topic describes guidelines on remote work. Internal controls are implemented to ensure that all information transfer is via Private Network (VPN).

1.3.9 Backup Policy

This topic describes guidelines on managing backup routines in order to ensure data protection against loss of information. Internal controls are implemented to ensure backups are executed as listed in the policy, periodically tested, and securely stored.

1.3.10 Malicious Code Protection Policy

This topic describes guidelines on using tools to protect against malware threats. Internal controls are implemented to detect, respond and mitigate the threat immediately.

1.3.11 Policy for Management of Technical Vulnerabilities

This topic describes guidelines for managing internal and external vulnerabilities for the Senior Group.

Internal controls are implemented to ensure that vulnerabilities are detected and mitigated according to service levels agreed with the business. Penetration tests are performed periodically to detect systemic failures, being a secondary control for vulnerability detection tools.

1.3.12 Event Management Policy

This topic describes guidelines for managing information security events. Internal controls are implemented to ensure that all security events are centralized, managed and continuously monitored.

1.3.13 Software Development Policy

This topic describes guidelines on the secure development of applications, following market practices. Production environments are segregated from homologation and development environments, ensuring that only previously authorized people can modify them. Internal controls are implemented to ensure that application updates are carried out through change management and respecting the segregation of duties. The Senior Group implements technologies to carry out static tests (SAST) and dynamic tests (DAST) during the development process.

1.3.14 Incident Response Policy

This topic describes guidelines for preventing, handling and responding appropriately to information security incidents that may impact the institution's services or technological resources. In addition, the policy describes prioritization and severity rules regarding possible security incidents, procedures for communicating with authorities and customers, when necessary.

1.3.15 Business Continuity Policy

This topic describes guidelines, procedures and strategies to be carried out during possible contingency scenarios in line with the institution's purpose and strategic goals.
Disaster recovery tests are carried out every six months to ensure that the strategy is always up to date.
The Senior Group runs its workload on global cloud providers that follow consolidated norms and standards in the international certification market for its Data Center, in terms of security tier and business continuity plan. This workload has its backup replicated in at least two Data Centers, ensuring prevention of the risk of total data loss, having as its sole and exclusive premise the ability to recover data in the event of a catastrophe classified as ruin, considering the recovery time applied by these global players.
A public version is available to all customers and industry: https://www.senior.com.br/politica-de-seguranca-da-informacao

1.4 HOW DOES THE INFORMATION SECURITY AWARENESS PROCESS TAKE PLACE

The Senior Group periodically holds training and awareness events on the subject of Information Security and Data Privacy, for all employees and third parties.

Below is a list of awareness processes:

• Onboard Training;

• Information Security Week;

• Livestreams;

- Phishing campaigns;
- Posts on the corporate social network.

1.5 TO WHOM SHOULD THE INFORMATION SECURITY POLICY BE DISCLOSED?

The Information Security Policy is disclosed to all Senior Group employees, as well as third parties.

A public version is available to all customers and the industry: https://www.senior.com.br/politica-de-seguranca-da-informacao

1.6 INFORMATION SECURITY POLICY FOR SUPPLIERS

The Senior Group manages the organization's suppliers in a formal and structured manner. Therefore, it is necessary to accept the Information Security Policy for Suppliers, prior to signing the service provision contract, to be able to provide products/services to the Senior Group.

The Information Security Policy for Suppliers is available to everyone: https://d2nytdlptrqhdi.cloudfront.net/wp-content/uploads/2024/04/25180109/PL011.pdf

1.7 INFORMATION SECURITY POLICY FOR LICENSED CONSULTANTS

The Senior Group performs, in a formal and structured manner, the management of licensed consultants who act on behalf of the company. All consultants operate under a service provision contract, with confidentiality clauses and non-disclosure of information to which they may have access, as well as confidentiality clauses related to the topic of personal data privacy.

To ensure that all licensed consultants act in accordance with the Security Policy, audits are carried out by the Information Security team, at intervals agreed with the organization.

2. PRIVACY AND DATA PROTECTION

In this item, concepts related to the Data Privacy Policy will be presented, as well as issues that demonstrate the importance of its elaboration, implementation and disclosure.

2.1 DATA PROTECTION OFFICER

The Senior Group appointed a professional as Person in Charge of Personal Data Protection (DPO). This professional has the role of informing and advising the company on privacy matters, controlling compliance with the LGPD (General Data Protection Law) and internal policies, providing advice regarding the assessment of the impact of data protection and monitoring its performance, also serving as a connection with ANPD (National Data Protection Authority) on issues related to the processing of personal data. For more information regarding the DPO, access our website: https://www.senior.com.br/portal-de-privacidades.

2.2 WHAT IS THE DATA PROTECTION POLICY?

The Data Protection Policy is a formal document, approved by Senior Group's board of directions, which aims to implement the best personal data privacy practices, with the purpose of assigning responsibility, defining rights, duties, expectations of access and use, penalties and promoting an organizational educational culture of privacy of Senior Group's information, customers, suppliers and partners.

2.3 PRIVACY NOTICE

The privacy notice is a clear and objective communication, through which the Senior Group, acting as controller, makes it clear to the holder how the processing of personal data is carried out, what types of personal data are collected, the purposes for which it is collected, the legal hypothesis that authorizes its handling, the third parties with whom data can be shared and the measures that are adopted to protect them.

This privacy notice can be consulted at the following address: https://www.senior.com.br/politica-de-privacidade

2.4 COOKIE POLICY

The Senior Group provides its titles, clients, suppliers and the market with a Cookies Policy, the purpose of which is to learn how users interact with the content, identify which resources are most sought after, count the visitors to a

page and improve the experience for the visitor.

The Cookie Policy can be consulted at the following address: https://www.senior.com.br/politica-de-cookies

2.5 CONTACT WITH HOLDERS

The Senior Group provides a form on its websites for data subjects to contact the company and/or request that their rights be exercised, including:

• Confirmation of the existence of data handling;

• Access to data;

• Correction of incomplete, inaccurate or outdated data;

• Anonymization, blocking or deletion of unnecessary, excessive or processed data that does not comply with the provisions of the LGPD;

• Data portability;

• Deletion of personal data processed without the consent of the data subject, except in the cases provided for in art. 16 of the Law;

• Information from public and private entities with which the Senior Group has shared data;

• Information about the possibility of not providing consent and the consequences of refusal;

• Revocation of consent.

The contact form with the Data Protection Officer can be consulted at the following address: https://www.senior.com.br/portal-lgpd

2.6 MAPPING OF PERSONAL DATA AND PROCESSING ACTIVITIES RECORD (ROPA)

Data mapping, or data inventory, data mapping or data flow, is a document that reflects the path taken by personal data within the organization, including processes, procedures and technologies through which the data passes.
The Senior Group keeps a data inventory and updates it constantly, as well as keeping a Record of Processing Activities (ROPA), in order to show how data is collected, what processing operations are carried out and how personal data is deleted.

2.7 PERSONAL DATA IMPACT ANALYSIS (AIPD)

The Data Protection Impact Assessment (DPIA), or even, Impact Report on Data Protection (RIPD), is a report whose function is to demonstrate how the Senior Group assesses risks in personal data processing operations and adopts measures to mitigate them.

3. COMPLIANCE AND CERTIFICATIONS

The Senior Group, as a way of demonstrating its commitment to the subject, implements, maintains and continuously improves the Information Security Management System (SGSI).

3.1 ISO 27001

The ISO 27001 standard is the international standard and reference for Information Security management. Its general principle is that the organization adopts a set of requirements, processes and internal controls with the aim of managing and mitigating risks.
The Senior Group has its Information Security Management System (ISMS) certified by the ISO 27001 standard, with the following scope: **Information Security Management System that supports Infrastructure, Application Development, Delivery and Maintenance of SaaS solutions**.

Below is the list of controls implemented by the organization:

3.1.1 Information Security Policy

The Senior Group maintains an Information Security Policy, disclosed internally and trained by all employees. This document is restricted to employees and describes all practices and the conduct that must be followed during professional activities by the company.

3.1.2 Information Security Organization

The Senior Group has implemented and continually improves a management structure to initiate and control the implementation and operation of information security within the company.

3.1.3 Security in Human Resources

The Senior Group has internal human resources processes to ensure that employees and external parties understand their responsibilities and comply with the roles for which they were selected.

3.1.4 Asset Management

The Senior Group has adequate processes and tools to identify the organization's assets and define the appropriate responsibilities for their protection.

3.1.5 Access Control

The Senior Group has implemented, operates and continuously improves the control process regarding access to information and information assets, with the aim of limiting access by unauthorized persons. Access management is carried out respecting the principle of segregation of functions for the following controls:

• Concession of accesses;

• Cancellation of accesses;

• Review of accesses;

• Revocation of accesses;

3.1.6 Encryption

Senior Group implements cryptographic controls to protect its information and information assets and ensure effective and appropriate use to maintain confidentiality, authenticity and integrity of information.

3.1.7 Physical and Environmental Security

The Senior Group has implemented, operates and continuously improves physical access controls to prevent unauthorized access, damage and interference with the organization's information and information processing resources.

3.1.8 Security in Operations

The Senior Group continuously implements and improves its internal processes to guarantee the safe and correct operation of information processing resources. The following technical controls and processes are implemented to ensure security in the organization's operations:

• Change Management;

• Capacity Management;

• Malware Protection;

• Security Copies (Backup);

• Registration and monitoring of events (logs);

• Technical vulnerability management;

• Operational compliance audits.

3.1.9 Communications security

The Senior Group implements technical controls that ensure the protection of information on networks and the information processing resources that support them. The following technical controls and processes are implemented to ensure security in communication services:

• Network access controls;

• Segregation of networks;

• Policies for transferring information;

• Security in electronic messages (emails);

• Contractual clauses of confidentiality and non-disclosure of information.

3.1.10 Information Systems Security Requirements

The Senior Group continuously implements and improves requirements to ensure that information security is an integral part of the entire lifecycle of information systems. Technical controls and processes are implemented to ensure security throughout the application lifecycle, namely:

• Analysis and specification of information security requirements;

• Application transaction protection;

• Policy for secure software development;

• Critical analysis of operational changes;

• Segregation between environments;

• Static and dynamic testing of applications.

3.1.11 Relationship in the Supply Chain

The Senior Group has implemented and continuously improves the relationship process with suppliers, with the aim of guaranteeing the protection of the organization's information and information assets.

As a good operating practice, the organization has created and keeps up to date an information security policy for suppliers, which can be consulted at the following address: https://d2nytdlptrqhdi.cloudfront.net/wp-content/themes/senior2019/content/pdf/PL011.pdf

3.1.12 Management of Information Security Incidents

The Senior Group has implemented and continuously improves an incident response process, with the aim of ensuring a consistent and effective approach to managing information security incidents, including communication about weaknesses and information security events.

3.1.13 Continuity of Information Security

The Senior Group has implemented and continuously improves an operational continuity process for technology environments, with the aim of ensuring that operations remain resilient after an impact.

3.1.14 Compliance

The Senior Group has implemented internal controls to ensure compliance with legal, statutory or contractual obligations related to information security and any security requirements. The ISO 27001 certificate was issued by the certified body Bureau Veritas, with international acceptance by the UKAS (United Kingdom Accreditation Service) seal.

3.2 SOC 1 Type II

The SOC 1 report assesses the structure of the company's internal controls, focused on financial auditing, that is, those that involve, in some way, the financial balance of customers. It is measured under three aspects:

• Access Management;

• Change Management;

• IT Operations Management.

The Senior Group has the SOC 1 Type II report, issued by Independent Audit, for the **HCM (Human Capital Management) product in SaaS**.

4. FAQ (Frequently Asked Questions)

Below are some questions asked by our customers regarding our information security and data privacy structure:

Question	Answer
1. Does the Senior Group have any other certification in addition to ISO 27001 and SOC 1 type II?	Yes. Senior has a Quality Management System certified by ISO 9001.
2. Does the Incident Response process include personal data?	Yes. It includes personal data and communication with holders and national authority, if necessary.
3. Does the Senior Group have an area responsible for Information Security?	Yes. The Senior Group has a corporate Information Security team, responsible for the topic within the organization.
4. Is confidential and sensitive information transmitted securely?	Yes. All information is transferred securely using the latest encryption protocols.
5. Is there a formal approval process for granting and using privileged users (administrators)?	Yes. Internal controls are implemented to ensure the segregation of duties in granting privileged access.
6. Are penetration tests performed? Are they outsourced or in-house?	Yes. Penetration tests are periodically contracted with third parties for Senior Group's cloud products. In addition, the internal offensive security team performs daily tests on applications and internal networks of the company.
7. Are logs recorded and stored for all internal systems and cloud systems?	Yes. All of the company's systems generate logs. All logs are centralized in a SIEM tool, with retention time agreed with the business.
8. Is there a formal process for the discarding of information, both sensitive and confidential?	Yes. The Senior Group has a formal process for discarding information, both physical and digital, for both its own information and that of customers.
9. Does the Senior Group have a backup policy implemented and disseminated among all technology environments?	Yes. All cloud technology environments have a backup policy implemented, with periodic integrity tests.
10. Does the Senior Group have a governance policy implemented and disclosed internally?	Yes. A governance policy for cloud environments is implemented and disclosed for all products sold by the Senior Group.
11. Does the Senior Group manage all suppliers?	Yes. An internal supplier management policy is implemented and adopted by the organization. Suppliers are registered, qualified based on risk and continuously monitored.
12. What frameworks are used by the Senior Group?	CIS Controls and NIST are used.
13. What professional information security certifications does the information security team have?	The information security team has qualified professionals in their roles, and has the following certifications: CISSP, CEH, OSCP, Lead Auditor ISO 27001/27701, Comptia Security+, Data Protection Officer, ITIL Specialist, COBIT, LPI3, DCPT, among others.

14. Is information security maturity evaluated periodically by third parties?	Yes. An information security maturity assessment is carried out annually with a third-party company, using the CIS Controls and NIST frameworks as a basis.
15. Are there contractual clauses with employees, third parties and suppliers on confidentiality, information security and data privacy?	Yes. All Senior Group contracts have confidentiality, security and privacy clauses.
16. Does the Senior Group have exclusive committees to deal with data security and privacy?	Yes. The Cloud Security Committee and the Data Privacy Committee.
17. Does the Group comply with the GDPR?	No. Senior Group companies have adapted their operations to comply with the General Data Protection Law (LGPD).
18. Does the Senior Group ever transfer personal data to other countries?	Yes. In order to fulfill a contract with customers, in some products, personal data may be transferred outside Brazil.