Information Security Policy

Administrative

Guidelines and Rules

SANTOS BEVILAQUA ADVOGADOS

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar

CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro

Rua Lauro Muller, 116, sala 1903

CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Summary

1. INTRODUCTION 5

1.1 PRESENTATION 5

1.2 OBJECTIVE 5

1.2.1 Application/Scope 5

2. REFERENCES AND REGULATIONS 6

3. GENERAL GUIDELINES 7

4. INFORMATION SECURITY COMMITTEE - ISC 8

4.1 INFORMATION SECURITY COMMITTEE (ISC) ORGANIZATION 8

4.2 GUIDELINES FOR INCIDENT NOTIFICATION 9

5. SECURITY IN HUMAN RESOURCES 10

5.1 SPECIFIC RESPONSIBILITIES 11

5.1.1 Personnel in General 11

5.1.2 Personnel under Exceptional Regime (Temporary Staff) 12

5.1.3 People and/or Process Manager 12

5.1.4 Data Protection Officer (DPO) 13

5.2 MONITORING AND AUDITING OF THE ENVIRONMENT 13

5.3 AWARENESS AND TRAINING 14

5.4 USE OF EMAIL 14

5.5 INTERNET USAGE 16

5.5.1 Monitoring and Ownership 16

5.5.2 Information Security and Responsibilities 16

5.5.3 Personal Use of the Internet 17

5.5.4 Specific Usage Guidelines 17

5.5.5 Specific Applications 18

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.6 USE OF SOCIAL MEDIA 19
5.7 USE OF MESSAGING SOFTWARE 19
5.8 USE OF COMPUTERS AND TECHNOLOGICAL RESOURCES 19
5.8.1 Maintenance and Updates 19
5.8.2 Antivirus and Incident Reporting 20
5.8.3 Data Transfer and Storage 20
5.8.4 Network Use and Security 20
5.8.5 Guidelines for the Use of Computers and Equipment 21
5.8.6 Prohibited Uses of Computers and Technological Resources 22
5.8.7 Use of the Corporate Network 22
6. ACCESS SECURITY (LOGICAL AND PHYSICAL) 23
6.1 PHYSICAL ACCESS MANAGEMENT 23
6.2 IDENTITY MANAGEMENT, LOGICAL ACCESS, AND PASSWORD CONFIGURATION 24
6.2.1 Responsibility and Use of Identification Devices 24
6.2.2 Login and Password Sharing 24
6.2.3 Password Requirements and Management 24
6.2.4 Access Blocking and Password Recovery: 25
6.2.5 Access Revocation Process 25
7. DATA SECURITY 26
7.1 INFORMATION AND DATA CLASSIFICATION 26
7.1.1 Information Security and Responsibilities 26
7.1.2 Monitoring and Reclassification 27
7.2 RESPONSIBLE PARTIES FOR CLASSIFICATION REQUESTS 27
7.3 PARTIES RESPONSIBLE FOR RECLASSIFICATION DEMANDS 28
7.4 CLASSIFICATION LEVELS 28
7.5 INFORMATION LABELING 29

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.5.1 Document and Media Labeling 30
7.5.2 Verbal Transmission of Information 30
7.5.3 Digital Storage 30
7.6 Information Handling 30
7.6.1 Handling of Physical Documents 31
7.6.2 Unforeseen Scenarios 31
8. SECURITY OF TECHNOLOGICAL RESOURCES 34
8.1 Minimum Security Requirements for Corporate Technological Resources 34
8.1.1 Monitoring and Incident Prevention: 34
8.2 Encryption 35
8.3 Log and Audit Trail Management 35
8.4 Backup Management 35
9. INFORMATION SECURITY SUPPORT (ACCESS MANAGEMENT AND SERVICE DESK) 37
10. COMPLEMENTARY INTERNAL GUIDELINES, TERMS, AND PROCEDURES 38
11. SANITIZATION 38
11.1 Sanitization Routine – SBA 39
11.1.1 Sanitization of Physical Documents 39
11.1.2 Sanitization of Equipment 40
12. VIOLATIONS AND SANCTIONS 41
12.1 Disciplinary Procedures and Violations 41
12.2 Sanctions and Responsibilities 41
12.3 Violation Detection and Reporting 42
13. VALIDITY AND REVIEW 42
14. VERSION CONTROL 42
15. FINAL PROVISIONS 43

1. Introduction

1.1 Presentation

The purpose of the Information Security Policy (ISP) of Santos Bevilaqua Advogados is to establish clear guidelines, controls, and principles to protect its informational assets, with a focus on minimizing risks and continuously improving the Information Security Management System (ISMS). It must, therefore, be followed and applied across all areas of the firm.

1.2 Objective

This Information Security Policy (ISP) aims to ensure the confidentiality, integrity, and availability of information—that is, to prevent access by unauthorized individuals, ensure that data is not altered or corrupted, and guarantee that information is always accessible when needed.

- ⇒ **Integrity:** Assurance that information is maintained in its original state, aiming to protect it—whether in storage or transit—against unauthorized, intentional, or accidental alterations.
- ⇒ **Confidentiality:** Assurance that access to information is granted only to authorized persons.
- ⇒ **Availability:** Assurance that authorized users have access to information and related assets whenever needed.

1.2.1 Application/Scope

This policy applies to all users who have access to information at Santos Bevilaqua Advogados, regardless of their relationship with the firm. To protect the firm's information, each individual (partners, associates, directors, managers, employees under CLT, and service providers) must:

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

⇒ Ensure the security of the information under their responsibility.

⇒ Be familiar and comply with the Information Security Policy (ISP) and internal rules.

⇒ In case of doubts, seek guidance from the Management.

2. References and Regulations

This Security Policy was developed in accordance with the following regulatory guidelines:

⇒ Law No. 13,709/2018 - Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados* - LGPD): Regulates the processing of personal data, including rules for the collection, use, storage, sharing, and deletion of data.

⇒ Decree no. 8,771/2016: Regulates the Internet Civil Framework and establishes guidelines for the security of communication networks and the handling of data.

⇒ Resolution no. 5,956/2021 of the National Agency of Telecommunications (*Agência Nacional de Telecomunicações* - Anatel) Sets forth cybersecurity requirements for telecommunications networks.

⇒ Technical Standards of the Brazilian Association of Technical Standards (*Associação Brasileira de Normas Técnicas* - ABNT) A set of standards that establish guidelines and requirements for various aspects of information security, such as NBR ISO/IEC 27002:2022, which addresses the information security management system.

⇒ European Regulation – General Data Protection Regulation GDPR): GDPR 2016/679 is a European legislation that addresses issues related to privacy and the protection of personal data. Created in 2018, this regulation applies to all individuals within the European Union and the European Economic Area. Additionally, it establishes guidelines for the transfer of personal data outside these regions.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

It is important to emphasize that this Security Policy is continuously updated to comply with new legislation and best practices in information security. For more information about the mentioned regulatory statements, please consult the following links:

⇒ Law no. 13,709/2018 (LGPD): https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

⇒ Decree no. 8,771/2016: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm

⇒ Resolution no. 5,956/2021 of Anatel https://www.anatel.gov.br/legislacao/resolucoes/2021/1435-resolucao-no-5956

⇒ Technical Standards of ABNT https://www.abnt.org.br/

⇒ General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

3. General Guidelines

Santos Bevilaqua Advogados clearly establishes that all data generated, processed, transmitted, or stored by its staff are intellectual property assets of the firm.

The manner in which this information is presented—whether physical, electronic, written, or spoken—and the way it is shared, stored, or transmitted do not change its fundamental purpose: the information must be used exclusively for authorized purposes. The firm implements and maintains ongoing information security efforts to protect the data under its management.

Security guidelines are strictly followed and monitored to ensure adequate and effective protection. Santos Bevilaqua Advogados reserves the right to monitor, audit, block, or back up any data or information in its possession that transits through its network, or any type of physical or logical access to its systems and environments.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

It is further established that the firm's IT equipment, communication devices, systems, and information must be used by the staff solely in the course of their professional activities. The firm's Management may implement measures to monitor the use of systems and services in order to ensure the security of the information being used.

4. Information Security Committee - ISC

The committee is responsible for defining, coordinating, and making relevant decisions, as well as deliberating on key aspects of information security, ensuring that projects and initiatives are understood, assessed, and prioritized.

4.1 Information Security Committee (ISC) Organization

The Information Security Committee (ISC) is formally composed of members of the staff with a minimum managerial level, appointed to participate in the group for a period of one year.
The ISC meetings will be held at least twice a year. Additionally, the ISC will convene on other occasions whenever there is a need to discuss serious incidents or make important decisions for Santos Bevilaqua Advogados.

The ISC will engage specialists, either internal or external, to support matters that require specific technical expertise.

It is the responsibility of the ISC:

- ⇒ To publish and promote the versions of the Information Security Policy (ISP) and the Information Security Standards approved by the ISC itself.
- ⇒ To propose investments related to information security with the aim of reducing risks.
- ⇒ To propose changes to the versions of the ISP and the inclusion, elimination, or modification of complementary standards.
- ⇒ To assess security incidents and propose corrective actions.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

⇒ To define appropriate measures in cases of non-compliance with the ISP and/or the complementary Information Security Standards.

⇒ To maintain the security of systems and IT infrastructure by performing continuous monitoring and periodic audits.

4.2 Guidelines for Incident Notification

Santos Bevilaqua Advogados adopts guidelines to prepare for and respond to security incidents in a swift, organized, and efficient manner, minimizing the consequences for all parties involved.

The level of response will depend on the amount of data and the complexity of the treatment applied.

What is a Security Incident?

A security incident is an unexpected situation that disrupts normal operations. In the context of data protection, it refers to any event that puts at risk the personal data of individuals who interact with the law firm. The National Institute of Standards and Technology (NIST) defines a security incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

The Brazilian General Data Protection Law (LGPD) establishes, in its Article 46, that data processing agents must adopt security measures, both technical and administrative, to protect personal data. The objective is to prevent unauthorized access and accidental or unlawful situations, such as destruction, loss, alteration, disclosure, or any other form of improper or unlawful processing.

Furthermore, Article 48 of the Brazilian General Data Protection Law (LGPD) states that the controller must notify the National Data Protection Authority (ANPD) and the data subject of any security incident that may pose a risk or significant harm. This communication must be made within a reasonable timeframe, and must contain, at a minimum:

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

- ⇒ A description of the nature of the personal data affected.
- ⇒ Information about the data subjects involved.
- ⇒ An indication of the technical and security measures used to protect the data, safeguarding trade and industrial secrets.
- ⇒ The risks related to the incident.
- ⇒ The reasons for any delay, if the communication was not immediate.
- ⇒ The measures that have been or will be taken to reverse or mitigate the effects of the damage.

In summary, the guidelines aim to establish a clear and effective protocol for managing security incidents, ensuring the protection of personal data and compliance with the LGPD.

5. Security in Human Resources

For the sake of information consistency, the Information Security Policy (ISP) will be communicated to all employees of Santos Bevilaqua Advogados, ensuring that the policy is followed both inside and outside the office.

The inclusion of the Confidentiality Agreement or Confidentiality Clause is an essential condition in all contracts of Santos Bevilaqua Advogados. Only with this guarantee of confidentiality will access to the information assets available at the firm be permitted.

Responsibility regarding information security will be communicated during the employee hiring process. Everyone must be guided on security procedures and the proper use of assets to minimize potential risks. Additionally, they are required to sign a responsibility agreement.

Production environments are segregated and strictly controlled, ensuring the necessary isolation from development, testing, and staging environments, when applicable.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Create and implement appropriate controls, audit trails, or activity logs at all relevant points and systems. This includes areas such as workstations, laptops, internet access, email, and commercial and financial systems, whether developed internally or externally.

Santos Bevilaqua Advogados disclaims all liability arising from the improper, negligent, or reckless use of the resources and services granted to its staff, reserving the right to analyze data and evidence for the purpose of obtaining proof to be used in investigative processes, as well as to take appropriate legal measures.

The maintenance of key systems and services is periodically tested to reduce the risks of loss of confidentiality, integrity, and availability of information assets.

The Information Security Policy (ISP) will be enforced at Santos Bevilaqua Advogados through specific procedures, mandatory for all employees regardless of hierarchical level, organizational role or employment or service relationship.

Failure to comply with the requirements set forth in this Information Security Policy (ISP) and the Information Security Standards will constitute a violation of the firm's internal rules and will subject the user to appropriate administrative and legal measures.

5.1 Specific Responsibilities

5.1.1 Personnel in General

Personnel is understood to be any individual—partners, associates, directors, managers, employees under the CLT labor law, lawyers, service providers through legal entities or not—who performs any activity inside or outside the firm.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Each person shall be fully responsible for any loss or damage they may suffer or cause to Santos Bevilaqua Advogados and/or third parties as a result of non-compliance with the guidelines and standards herein referred to.

5.1.2 Personnel under Exceptional Regime (Temporary Staff)

They must understand the risks associated with their special status and strictly comply with the terms set forth in the acceptance granted by the Information Security Committee (ISC).
The concession may be revoked at any time if it is determined that the business justification no longer justifies the risk associated with the exceptional regime, or if the person who received it fails to comply with the conditions defined in the acceptance.

5.1.3 People and/or Process Manager

Maintain an exemplary attitude regarding information security, serving as a role model for the persons under their management.

Assign to the staff, during the hiring phase and formalization of individual employment, internship, service provision, or partnership contracts, the responsibility to comply with the Information Security Policy (ISP) of Santos Bevilaqua Advogados. Require the staff to sign the Commitment and Acknowledgment Agreement, undertaking the duty to comply with the established rules and committing to maintain secrecy and confidentiality—even after termination—regarding all information assets of Santos Bevilaqua Advogados.

Before granting access to the firm's information, require casual staff and service providers who is not covered by an existing contract to sign a Confidentiality Agreement, for example, during the data collection phase for the submission of commercial proposals.

By virtue of the privileges inherent to their roles, administrators and operators of computer systems have the ability to access files and data of other users. However, such access is restricted to situations where it is necessary for the performance of operational activities under their

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

responsibility, such as computer maintenance, backup operations, audits, or environment testing,

to ensure the integrity of audit records and prevent fraud, segregate administrative and operational functions. This measure aims to restrict each individual's powers to the minimum necessary, eliminating or at least reducing the existence of persons who could delete logs and audit trails of their own actions.

The security of systems with public access must be treated with special attention, implementing robust protection measures and ensuring the preservation of evidence that allows traceability of actions for audit or investigation purposes, if necessary.

5.1.4 Data Protection Officer (DPO)

Santos Bevilaqua Advogados has appointed a Data Protection Officer (DPO) to play a key role in the data protection process, particularly in responding to information security incidents. The DPO will serve as the communication link between the firm, the data subjects, and the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados* - ANPD), ensuring compliance with the LGPD.

Their main responsibilities include:
Facilitating Communication: Acting as a liaison between the incident response technical team and management. This ensures that the plan is properly followed and that all actions are in compliance with the requirements of the LGPD. The DPO ensures that data subjects are informed clearly and transparently about any incidents that may affect their personal data.

5.2 Monitoring and auditing of the environment

To ensure compliance with the rules mentioned in this ISP, Santos Bevilaqua Advogados may:

⇒ Implement monitoring systems on workstations, servers, email, internet connections, mobile or wireless devices, and other network components. The information generated

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

- ⇒ by these systems may be used to identify users and their respective accesses, as well as the materials handled.
- ⇒ Make public the information obtained from monitoring and auditing systems in cases of judicial requirement, request by management or the partners' committee, or by order of the Information Security Committee.
- ⇒ Conduct inspections at any time on machines owned by the firm.
- ⇒ Install preventive and detectable protection systems to ensure the security of information and access perimeters.

5.3 Awareness and Training

Promote periodic training and awareness initiatives focused on Information Security for the staff, third parties, and service providers.

More information can be found in the "*Information Security Awareness Training*"

5.4 Use of email

The purpose of this policy is to inform the staff of Santos Bevilaqua Advogados about the permitted and prohibited activities regarding the use of corporate email. The use of the Santos Bevilaqua Advogados email system is intended strictly for business purposes related to the user's professional activities within the firm. Personal use of this service is allowed as long as it is done sensibly, does not interfere with the firm's operations, and does not harm the office in any way.

Santos Bevilaqua Advogados reserves the right to track, monitor, record, and inspect any information transmitted via corporate email.

Personnel are strictly prohibited from using the Santos Bevilaqua Advogados email system to:

- ⇒ Send unsolicited messages to multiple recipients, except when related to legitimate office use.
- ⇒ Send any message by electronic means that could make the sender and/or the firm or its departments vulnerable to civil or criminal liability.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

- ⇒ Disclose unauthorized information or share screenshots, systems, documents, or similar materials without the express and formal authorization granted by the owner of the information asset.
- ⇒ Falsify addressing information or alter headers to conceal the identity of senders and/or recipients, with the intent of avoiding applicable penalties.
- ⇒ Delete relevant email messages when any of the office's departments is subject to any type of investigation.
- ⇒ Produce, transmit, or disseminate messages that contain any act or guidance that conflicts with or opposes the interests of Santos Bevilaqua Advogados.
- ⇒ Include electronic threats such as spam, mail bombing, or computer viruses.
- ⇒ Contain files with executable code (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) or any other extension that poses a security risk.
- ⇒ Seek unauthorized access to another computer, server, or network.
- ⇒ Attempt to disrupt any service, server, or computer network through any illicit or unauthorized method.
- ⇒ Attempt to bypass any security system.
- ⇒ Intend to secretly monitor or harass another user.
- ⇒ Attempt to access confidential information without the explicit authorization of the partners.
- ⇒ Attempt to improperly access information that could cause harm to any individual.
- ⇒ Include encrypted or otherwise masked images.
- ⇒ Contain attachments exceeding 30 MB for sending (internal and internet) or 30 MB for receiving (internet).
- ⇒ Contain content deemed inappropriate, obscene, or illegal.
- ⇒ Be slanderous, defamatory, degrading, infamous, offensive, violent, threatening, pornographic, etc.
- ⇒ Contain discriminatory harassment based on gender, race, physical or mental disability, or other protected categories.
- ⇒ Have local or national political purposes (political propaganda).
- ⇒ Include material protected by copyright without permission from the right holder.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Email messages must always include a signature in the following format:

⇒ Person's Name

⇒ Office Logo

⇒ Unit Address

⇒ Phone Number(s)

⇒ Office Website Link

5.5 Internet Usage

Santos Bevilaqua Advogados has established a set of rules to promote the ethical and professional use of the internet by its staff. While connection to the corporate network offers significant benefits, it also poses substantial risks to the firm's information assets.

5.5.1 Monitoring and Ownership

Any information accessed, transmitted, received, or produced on the internet through the firm's network is subject to disclosure and auditing. Therefore, Santos Bevilaqua Advogados, in full legal compliance, reserves the right to monitor and log all access.

The equipment, technology, and services providing internet access are the property of the firm. This means the firm may review and, if necessary, block any file, website, email, domain, or application stored on the network or the internet (whether on a local disk, workstation, or private network areas) to ensure compliance with its Information Security Policy.

5.5.2 Information Security and Responsibilities

Monitoring of the internal network aims to ensure the integrity of data and software. Any attempt to alter security parameters without proper credentials and authorization will be considered inappropriate, and the associated risks will be communicated to the associate and their manager.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

The use of resources for illicit activities may result in administrative actions and civil or criminal penalties, with the firm actively cooperating with the competent authorities.

5.5.3 Personal Use of the Internet

Internet access provided by the firm may be used for personal purposes, provided that:

- ⇒ It does not interfere with the progress of work within the departments.
- ⇒ It does not compromise network bandwidth during business hours.
- ⇒ It does not disrupt the proper flow of activities.
- ⇒ It does not present a conflict of interest with the firm's business objectives.

This means that browsing news or service websites, for example, is acceptable, as Santos Bevilaqua Advogados supports its associates in staying well-informed.

5.5.4 Specific Usage Guidelines

Images and Copyrights: Only personnel authorized by the firm may copy, capture, print, or send screen images to third parties, and must comply with the internal image usage policy, the Copyright Law, the image protection guaranteed by the Federal Constitution, and other applicable legal provisions.

Confidential Information: The disclosure or improper sharing of information from the administrative area in discussion lists, websites or social communities, chat rooms, instant messaging platforms, or any other similar internet technology is strictly prohibited.

Downloads: Staff with internet access may only download programs directly related to their activities at the firm. License compliance and proper registration of these programs must be ensured, with prior authorization from Management.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Unauthorized/Pirated Software: The installation, copying, or distribution of unauthorized software protected by copyright, trademark, or patent over the internet is strictly forbidden. Any unauthorized software downloaded will be removed by the Systems Management team. Under no circumstances may firm resources be used to download or distribute pirated software or data, which is considered a crime.

Sensitive Content: Materials of a sexual nature shall not be displayed, stored, distributed, edited, printed, or recorded using any resource. If strictly necessary for a specific user profile, security groups must be created and their members designated by management.

Uploading Firm Data: The staff with internet access may not upload licensed software or firm-owned data to partners or clients without the express authorization of the responsible party.
Viruses and Threats: It is prohibited to use firm resources to intentionally propagate any kind of virus, worm, trojan horse, spam, harassment, disruption, or remote-control programs.

5.5.5 Specific Applications

The following are not allowed:

- ⇒ Access to peer-to-peer software (such as Kazaa, BitTorrent, and similar platforms).
- ⇒ Access to proxy websites.

Streaming services (online radios, broadcast channels, and the like) will be allowed only for specific groups.
Instant messaging services (Microsoft Teams, WhatsApp, and similar) will initially be allowed but may be blocked if formally requested by management to the partners' committee.
These guidelines ensure that the digital environment of Santos Bevilaqua Advogados is used in a secure, ethical, and lawful manner, safeguarding both the firm’s assets and its clients' data.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.6 Use of Social Media

All matters related to external communication and social media are centralized in the marketing, communications, or other formally authorized departments. Consequently, no employee, third party, service provider, and/or partner is authorized to publish, comment, or engage in similar behaviors on behalf of Santos Bevilaqua Advogados—whether through communications, social media, or external websites—without proper authorization.

5.7 Use of Messaging Software

Santos Bevilaqua Advogados authorizes the use of the Microsoft Teams tool for internal communication among its personnel. However, transferring or sharing files or any confidential information outside the corporate network is strictly prohibited.

5.8 Use of Computers and Technological Resources

At Santos Bevilaqua Advogados, the guidelines for the use of IT equipment and resources aim to ensure security, data integrity, and the proper use of the firm's assets. The staff must handle equipment appropriately and follow operational procedures.

5.8.1 Maintenance and Updates

All maintenance, installation, uninstallation, configuration, or modification procedures involving equipment and systems are the sole responsibility of the IT Support department. Security updates and patches may only be applied after validation in a testing environment and official release by the manufacturer.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.8.2 Antivirus and Incident Reporting

All systems and computers must have antivirus software installed, active, and continuously updated. In the event of suspected viruses or functional issues, users must contact the technical department by opening a ticket through the service desk.

5.8.3 Data Transfer and Storage

Software Transfer: The transfer or disclosure of any software or program to third parties is only permitted after proper identification of the requester and positive verification, in accordance with the classification of the information and the actual need of the recipient.

Personal Files: Personal files (photos, music, videos, etc.) must not be copied to network drives to avoid server overload. If identified, such files may be permanently deleted after prior notice to the user.

Essential Documents: Documents critical to the firm's activities must be saved on network drives. Files saved only locally (e.g., "C drive") are not backed up and may be lost in the event of computer failure, making the user solely responsible.

5.8.4 Network Use and Security

Personnel — especially those persons with privileged accounts — must not execute commands or run programs that may overload the corporate network without prior authorization from the Systems Management team. All corporate incidents, such as vulnerabilities, viruses, or cyberattacks, must be immediately reported to the Information Security team via email suporte@santosbevilaqua.com.br .

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.8.5 Guidelines for the Use of Computers and Equipment

The main guidelines for the proper use of computers and IT resources are:
Passwords: All individual computers must be password-protected to restrict unauthorized access. Passwords are set by the firm's Management, which will have access for maintenance purposes.
Unfamiliar Devices: All persons must report any unfamiliar device connected to the computer to suporte@santosbevilaqua.com.br

Handling and Repairs: It is prohibited to open or handle computers or other equipment for repairs unless performed by a technician of the firm's Management or authorized third-party service providers.
USB devices are blocked to prevent data transfers, thereby protecting the environment from unwanted programs or viruses. In exceptional situations, USB devices may be unblocked as a contingency, subject to the express authorization of the managers of the involved areas and with the IT team's awareness. Food and Smoking: The consumption of food, beverages, or smoking at the workstation and near the equipment is strictly prohibited;

Configuration and Security: Associates must maintain the configuration of the equipment provided by the firm, in accordance with information security policies and specific regulations, taking responsibility as custodians of the information.
Terminal Locking: Computer terminals and printers must be password-protected (locked) when not in use, in accordance with the Authentication Policy.

Default Passwords: Default passwords of technological resources acquired by the office must be changed immediately.

Event Logs: Equipment must securely preserve event logs, including user identification, access dates, and times.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.8.6 Prohibited Uses of Computers and Technological Resources

The use of Santos Bevilaqua Advogados' resources is prohibited in the following situations:

- ⇒ Attempting or obtaining unauthorized access to another computer, server, or network;
- ⇒ Bypassing security systems.
- ⇒ Accessing confidential information without explicit authorization from the partners.
- ⇒ Secretly monitoring other individuals through electronic devices or software (e.g., *sniffers*).
- ⇒ Interrupt services, servers, or networks by illegal or unauthorized methods.
- ⇒ Use technological resources to commit or be an accomplice in violations, sexual harassment, disturbance, manipulation, or suppression of copyrights or intellectual property without legal authorization.
- ⇒ Host pornography, racist material, or any other content that violates legislation, morality, good customs, or public order.
- ⇒ Use pirated software, which is considered a crime under national law.

5.8.7 Use of the Corporate Network

Santos Bevilaqua Advogados holds exclusive ownership of all material and digital assets, including software, documents, designs, and others, created by its personnel,
third parties, service providers, and partners, provided that the technological resources of the firm are used, regardless of the time of creation. By way of example, information, documents (whether in physical or digital format), creations, inventions, developments, improvements, or any other enhancements that are made, stored, produced, or transformed may be considered material and intellectual assets.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

All users are responsible for preserving the organization's intellectual property, as well as observing and respecting the intellectual property rights of third parties, in accordance with applicable law. In cases of omission, intent, or negligence, users may be held liable.

All information belonging to the firm, or made available by it, is for exclusive corporate use only. Its use for personal purposes, as well as its sharing with third parties, regardless of how it was obtained, inferred, or developed by the employee in their work environment, is strictly prohibited.

6. Access Security (Logical and Physical)

Personnel are responsible for all actions performed using their access credentials (whether physical or logical), including any activity on their workstation during their logged-in session. Credentials are personal and non-transferable.

6.1 Physical Access Management

Access Control: Access to the Datacenter is restricted to authorized personnel only. Visitors or third parties may only access it with prior authorization from the firm’s management and/or board and must be accompanied by an authorized staff member.
Surveillance: The building's security cameras monitor the premises. There must be two copies of the Datacenter door key. One copy shall remain with the person responsible for access to the environment, and the other shall be held by the firm’s management.
Fire protection: Implementation of fire detection and suppression systems to protect physical assets.
Environmental Control: The Datacenter must be kept clean and organized. Any procedure that generates waste or dirt in this environment may only be carried out with the collaboration of the General Services Department. The entry of any type of food, beverage, or flammable product is not permitted.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

6.2 Identity management, logical access, and password configuration

The protection of identities and passwords is fundamental at Santos Bevilaqua Advogados to prevent fraud and ensure information security. Access control is strict, following the principle of least privilege, where each individual accesses only what is essential for their functions.

6.2.1 Responsibility and Use of Identification Devices

The use of devices or passwords belonging to others is a crime (Art. 307 of the Penal Code). All identification devices in the office — such as badges, system access credentials, digital certificates, and biometric data — must be linked to a single individual and their official documents. The user is solely responsible for the proper use of these devices, both before the office and under the law.

6.2.2 Login and Password Sharing

Sharing any personal identification device is prohibited. If a login is shared, legal responsibility falls on the users who use it, unless the manager is aware of or has requested the sharing. Sharing logins for system administration functions is strictly forbidden.

6.2.3 Password Requirements and Management

System access is protected by strong authentication, including secure passwords and multi-factor authentication (MFA). Passwords for Users Without Administrator Privileges: A minimum of 12 alphanumeric characters, including special characters (@ # $ %), and a mix of uppercase and lowercase letters. Passwords for administrators or users with privileged access: A minimum of 12 alphanumeric characters, including special characters (@ # $ %) and a mandatory mix of uppercase and lowercase letters.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Passwords must not be:

⇒ Written down or stored in unencrypted electronic files.

⇒ Based on personal information (e.g., name, date of birth).

⇒ Obvious keyboard combinations (e.g., "abcdefgh").

⇒ Passwords must be changed every 90 days, without repeating any of the last 24 passwords. For critical systems and privileged logins, passwords must be changed every 30 days. Systems must enforce these changes within the established timeframes.

6.2.4 Access Blocking and Password Recovery:

All accesses will be immediately blocked when they become unnecessary. In the event of a member of the staff's departure, the HR Department must immediately notify the IT Department to block access. This rule also applies to terminated contracts or test users.

If a staff member forgets their password, they must formally request a new one from the system administrator via email. suporte@santosbevilaqua.com.br

6.2.5 Access Revocation Process

Termination	Unfavorable	Favorable Conditions
Revocation Timing	Immediate/abrupt upon termination notice.	Usually on the last day of work or gradually.
Risk Level	High	Low to moderate
Scope	Total and complete. No residual access.	Specific accesses may be temporarily maintained for transition purposes.
Monitoring	Potential for monitoring.	Generally, no intensive monitoring after notice.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Follow-up	Focused on threat mitigation.	Focused on a smooth transition.

7. Data Security

All information of Santos Bevilaqua Advogados is classified by assigning an appropriate level of protection according to its value, level of confidentiality, sensitivity, and criticality to the business **(least privilege principle)**. Data belonging to Santos Bevilaqua Advogados is handled and stored on official corporate computers and/or private cloud services.

It is not permitted to handle, store, or transfer data—without authorization—to external devices or storage platforms, such as third-party cloud services (Dropbox, OneDrive, iCloud, Google Drive, among others).

7.1 Information and Data Classification

To ensure the security and confidentiality of information, Santos Bevilaqua Advogados restricts access to only what is essential for each individual's duties.

7.1.1 Information Security and Responsibilities

Information belonging to Santos Bevilaqua, third parties, or its subsidiaries is classified according to its level of sensitivity. This classification determines the appropriate level of priority and protection. Responsibility for classification lies with the managers of each area or with an individual designated by them. Even if the task is delegated, final responsibility remains with the manager. The firm has designated change/transformation agents to assist in implementing the culture of information classification. However, it is the responsibility of each staff member to handle information in accordance with its classification level and the established guidelines.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.1.2 Monitoring and Reclassification

Periodically, the information classification and handling process may be monitored and measured to verify compliance, gather metrics, suggest improvements, and develop action plans. Classification requires careful analysis of factors such as:

⇒ The intrinsic value of the information.
⇒ Legal obligations
⇒ Level of sensitivity and criticality.
⇒ Validity period.
⇒ Needs for sharing and restrictions.
⇒ Involved risks.
⇒ Potential impact on the firm's business and reputation.

The person responsible for classification must conduct periodic critical reviews to ensure that the protection level remains appropriate, as classification may change over time. Information may be reclassified when:

⇒ An incorrect classification is identified.
⇒ Changes occur in the sensitivity context of the information during its lifecycle.
⇒ There is a need to comply with a legal requirement or changes in Santos Bevilaqua's internal processes.

7.2 Responsible Parties for Classification Requests

⇒ All users are responsible for reporting to the information manager any absence or inconsistency in the proper classification of information.
⇒ The responsibility for reclassifying (or not) the information lies with the manager.
⇒ External information involved in the processes of Santos Bevilaqua — such as third-party reports, client and supplier documents and data — is handled according to the level of criticality and sensitivity defined by the external party responsible.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

⇒ An agreement should be sought with third parties with whom information is exchanged to ensure the proper identification, classification, and handling of information between the organizations, aiming for secure information sharing.

⇒ The person responsible for receiving and/or sharing information from an external party must pay special attention to the interpretation of classification labels on the documents, as they may have different definitions for identical or similar labels to those used internally.

7.3 Parties Responsible for Reclassification Demands

All users are responsible for reporting to the information manager any absence or inconsistency in the proper classification of information; The responsibility for reclassifying (or not) the information lies with the manager.

7.4 Classification Levels

Below are the classification levels used at Santos Bevilaqua Advogados

Classification Levels	Characteristics
Public	Information classified as public is that which disclosure does not cause harm to Santos Bevilaqua Advogados, its clients, or partners. Such information may be freely shared with the general public, provided its integrity is preserved. Santos Bevilaqua Advogados reserves the right to designate a responsible party or department to manage the disclosure of this information. The responsibility for the proper classification of such information lies with the respective area manager.
Internal	Internal information of the firm is accessible to all staff members and service providers, provided they commit to maintaining the confidentiality of the information to which they have access.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Reserved	Confidential information refers to data whose access is restricted to a specific group of individuals, departments, or positions within Santos Bevilaqua Advogados. Access to such information is limited to those who require it to perform their professional duties. Examples of confidential information include projects, reports, indicators, and other similar documents.
Secret/Confidential	Information classified as Secret/Confidential requires special handling, as unauthorized disclosure or improper access may cause financial, legal, regulatory, or contractual harm, as well as damage to the reputation, image, or strategy of Santos Bevilaqua Advogados. Examples of Secret/Confidential information include personal data of individuals, supplier information, and strategic information of the firm.

7.5 Information Labeling

All information of Santos Bevilaqua Advogados is identified with at least the assigned classification level, the permitted access group, and the creation date. The identification of the information must clearly indicate the classification level and the access group.

Examples of materials that are labeled:

- ⇒ Documents
- ⇒ Files
- ⇒ Envelopes
- ⇒ Physical files
- ⇒ Electronic files
- ⇒ Electronic media
- ⇒ Conversations
- ⇒ Presentations

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.5.1 Document and Media Labeling

Reports (on screen, in files, or printed), system screens, electronic messages, and file transfers must display appropriate information classification labels. These labels should be clearly visible, at minimum, on the cover of documents, folders, or storage files. It is strongly recommended to label all pages of documents by adding headers or footers.

The person responsible for labeling is the same one who performed the classification process. If a document contains different classification levels, it must be classified and labeled according to the highest/most restrictive level present in the file.

7.5.2 Verbal Transmission of Information

In situations such as meetings or presentations, the person conveying information verbally must disclose the information's classification and necessary precautions at both the beginning and end of the event.

7.5.3 Digital Storage

Information stored on file servers and other storage devices must have a clear access group label. If it is a shared folder, it must be protected against unauthorized access. Digital documents must contain headers or footers indicating the information category.

7.6 Information Handling

Proper handling of information is essential to ensure its confidentiality, integrity, and availability, providing greater control and protection. All information must be treated with the same level of care, regardless of the person, position, or department.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.6.1 Handling of Physical Documents

Documents classified as confidential or secret in physical format must be stored in locked drawers or cabinets to prevent access by unauthorized individuals. When the workspace is unoccupied, these documents must be removed from desks and other visible areas. Internal, confidential, or secret information must not be left exposed on boards, whiteboards, or similar surfaces to prevent unauthorized viewing.

7.6.2 Unforeseen Scenarios

Guidelines for handling information, based on different scenarios and classification levels, are detailed in a specific reference table. If a scenario is not covered, the immediate manager must be consulted so the policy can be updated accordingly.

Classification Level				
Scenario	**Public**	**Internal**	**Confidential**	**Secret**
Logical or Physical Access	No Restrictions	Only for Santos Bevilaqua staff	Only for people within the access group	Only for people within the access group
Storage on printed media (paper, posters, etc.)	No Restrictions	Only for Santos Bevilaqua Advogados staff	Only for people within the access group	Only in areas with controlled physical access for the access group, in locations with restricted access (locked cabinets/drawers).
Storage in digital files (network):	No Restrictions	Only within the areas of Santos Bevilaqua Advogados	Only in areas with controlled physical access for the access group	Only on the file servers of Santos Bevilaqua Advogados with access control preferably with an additional level of security (e.g., encryption)
Storage on Digital Media (DVD, CD, USB drive, etc.)	No Restrictions	Only on the file servers of Santos Bevilaqua Advogados network	Only on the file servers of Santos Bevilaqua Advogados with access control	Only with authorization from a partner or area manager, and with strong password or encryption. Preferably, the media must be stored within the premises of Santos Bevilaqua Advogados, in a locked cabinet or drawer, and in locations with controlled physical access for the access group.

Reproduction (printed or digital)	No Restrictions	Media must be stored within the premises of Santos Bevilaqua Advogados.	Only with authorization from a partner or the area manager. Preferably, the media must be stored within the premises of Santos Bevilaqua Advogados, in a locked cabinet or drawer, and in locations with controlled physical access for the access group.	Only with authorization from the responsible manager.
Reproduction (printing)	No Restrictions	Only for Santos Bevilaqua Advogados staff	Only when the user accompanies the printing and ensures that no one will have access to the printed document. Use a password to release the print job, when the printer has this feature.	Only with authorization from the responsible manager, and the user must accompany the printing and ensure that no one will have access to the printed document. Use a password to release the print job, when the printer has these features.
Physical transportation	No Restrictions	No restrictions within the premises of Santos Bevilaqua Advogados. For transportation outside Santos Bevilaqua Advogados, authorization from the responsible manager is required.	Only with the use of seals, if the transportation is not performed by someone from the access group. Authorization from the responsible manager is necessary if the transport is outside the premises of Santos Bevilaqua Advogados, and the information must be stored in a protected location during the trip.	Only with the use of seals. If the transport is not carried out by someone from the access group, use a hand-delivery service. Transportation outside the premises of Santos Bevilaqua Advogados requires authorization from the responsible manager. Store the information in a protected location, preferably locked or in a safe, during the trip.
Transmission by e-mail	No Restrictions	Internal, no restrictions. For external recipients outside Santos Bevilaqua Advogados, authorization from the responsible manager is required.	Only for the access group. Outside the access group, authorization from the information partner is required.	Only for the access group. Outside the access group, authorization from the information partner is required. Additionally, protection techniques such as passwords and encryption are considered.

External digital transmission (FTP, link, internet, etc.)	No Restrictions	Only with authorization from the responsible manager.	Only with the authorization of the responsible manager and through Santos Bevilaqua Advogados' equipment.	Only with the authorization of the responsible manager and through Santos Bevilaqua Advogados' equipment, and in encrypted form.
Video/voice transmission	No Restrictions	Only for Santos Bevilaqua Advogados staff	Only for the access group.	Only for the access group and through Santos Bevilaqua Advogados' equipment.
Transmission during presentations	No Restrictions	Only for Santos Bevilaqua Advogados staff	Only for the access group. For individuals outside this group, only with the authorization of the responsible manager	Only for the access group. For individuals outside the access group, only with the authorization of the responsible manager
Disposal of digital and/or analog media	No Restrictions	Only within the areas of Santos Bevilaqua Advogados	The device must be physically destroyed, or the information must be destroyed, deleted, or overwritten using techniques that make the original information unrecoverable. Do not use only the standard delete or format functions.	The device must be physically destroyed, or the information must be destroyed, deleted, or overwritten using techniques that make the original information unrecoverable. Do not use only the standard delete or format functions.
Disposal of printed media	No Restrictions	Shred the information within the premises of Santos Bevilaqua Advogados.	Preferably, shred the information within the premises of the responsible department and in the presence of a member of the access group assigned to that information.	Preferably, shred the information within the premises of the responsible department and in the presence of a member of the access group assigned to that information.
Deletion of computer files	No Restrictions	Delete from the folder where it is stored.	Delete from the folder where it is stored and from the recycle bin as well.	Delete from the device's recycle bin and adopt technological solutions to ensure that the information cannot be recovered.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

8. Security of Technological Resources

It is strictly forbidden to use any Information Technology devices (such as servers, databases, routers, development software, etc.) that have not been previously approved and are not under the management of the IT or Information Security Department.

8.1 Minimum Security Requirements for Corporate Technological Resources

Corporate technological resources must have implemented at least the following, Server Security: Continuous monitoring to eliminate vulnerabilities and apply immediate security patches.

Network Segregation: Implementation of network segregation (physical or logical) using appropriate mechanisms and technologies to ensure the confidentiality, integrity, and availability of transmitted information.
Antivirus: Installation of antivirus software on all workstations, with defined procedures to ensure updates and proper operation.
Email Protection: Email protection solutions, including anti-spoofing, reputation filtering, AntiSpam, and anti-phishing.

- ⇒ Security Barriers: Equipment that establishes security barriers, such as Firewalls and Web Application Firewalls (WAF).
- ⇒ User Computer Security: User computers must have personal firewalls, security configurations, and patch updates to reduce the risk of intrusions, data leaks, and unauthorized access.

8.1.1 Monitoring and Incident Prevention:

Technological controls are implemented to monitor, protect, and minimize risks associated with information or processing assets, aiming to preserve confidentiality, integrity, and availability

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

These controls must function to prevent, restrict, monitor, and detect security incidents (e.g., NOC – Network Operations Center and SOC – Security Operations Center). Additionally, clocks in corporate environments and systems are synchronized with a precise, centralized time source.

8.2 Encryption

Disk encryption is mandatory on all office notebooks and mobile devices. This measure protects confidential information and prevents data leaks in the event of equipment loss or theft.

To safeguard company information, any externally hosted application must use the HTTPS protocol for communication and advanced encryption for data transmission.

The transmission of confidential information over the internet (via APIs, services, or partner communications) requires the implementation of dedicated encryption mechanisms. Cryptographic keys must be securely and centrally stored using password vaults or corporate key management software.

8.3 Log and Audit Trail Management

It is essential that all systems critical to the company have enabled auditing mechanisms. These mechanisms must record all privileged actions, such as system login and logout, device connection and disconnection, unauthorized access attempts, security breaches, and other relevant events.

The security of event logs and their resources requires protection against unauthorized access and tampering, ensuring the accuracy and confidentiality of the information.

8.4 Backup Management

All backups are automated through scheduling systems to preferably run outside business hours, during so-called "backup windows" periods when there is little or no user or automated process access to IT systems.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Personnel responsible for managing backup systems must frequently research updates for patches, new product versions, product lifecycle (when software is no longer supported by the manufacturer), improvement suggestions, among others.
Backup media (such as DAT, DLT, LTO, DVD, CD, and others) are stored in a dry, climate-controlled, secure location (preferably, if possible, in fireproof safes according to ABNT standards) and as far away as possible from the Datacenter.

Backup media are properly identified, including when it is necessary to rename them, using non-handwritten labels, providing a more organized and professional appearance.
The lifespan and usage of backup media must be monitored and controlled by the responsible personnel, aiming to discard media that may present recording or restoration risks due to prolonged use, as well as exceeding the manufacturer's recommended lifespan.

The need to renew media due to natural wear, as well as the existence of stock for any emergency use, is determined and controlled by those responsible for the activity.
Media showing errors should first be formatted and tested. If the error persists, the media must be destroyed (rendered unusable).

Historical or special backup media should be stored in secure facilities, preferably, if possible, with a vault room structure. Essential and critical backups for the smooth operation of Santos Bevilaqua Advogados' business require a special retention rule, as established in specific procedures and according to the Information Classification Standard, thereby complying with existing fiscal and legal regulations in the country.

In the event of a backup and/or restore error, the operation must be performed at the first available time once the responsible person identifies and resolves the issue.The executor must restore files to a different location than the original, to avoid overwriting valid files.

To formalize control over backup and restore executions, a strict control form must be used to record these routines, which shall be completed by the responsible personnel and audited by the infrastructure coordinator, according to the Backup and Restore Control Procedure.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Responsible personnel designated in the relevant procedures and responsibility spreadsheet may delegate the operational task to a custodian when, due to force majeure, they are unable to perform the operation. However, the custodian cannot exempt themselves from responsibility for the process.

9. Information Security Support (Access Management and Service Desk)

Santos Bevilaqua Advogados maintains a partnership with a specialized third-party company for information security support. This collaboration covers access management and the service desk, relying on expertise in information technology applied to the legal context.
The scope of activities includes the following demands:

- ⇒ Support and maintenance of machines;
- ⇒ Management of access to the company's systems and environments;
- ⇒ Managing and publishing the inventory of systems, machines, and access matrix;
- ⇒ Managing protection activities, coordinating, and communicating cybersecurity events;
- ⇒ Evaluation of security requirements in new projects;
- ⇒ Vulnerability Management and Detection;
- ⇒ Security incident response;
- ⇒ Support to the Information Security Committee for updates to policies, standards, and procedures related to Information Security (IS).

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

10. Complementary Internal Guidelines, Terms, and Procedures

Documents that comprise the Information Security and Privacy efforts of Santos Bevilaqua Advogados, without prejudice to other policies, terms, and standards not specified here, include:

⇒ Information Security Awareness and Training Actions – SBA

⇒ Incident Notification Guidelines – SBA

⇒ Information Security Incident Response Plan

⇒ Encryption Guidelines – SBA

⇒ Hardening Guidelines – SBA

⇒ Business Continuity Plan and Crisis Management

11. Sanitization

Sanitization aims to protect confidential information by ensuring compliance with privacy laws (LGPD) and maintaining data integrity.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

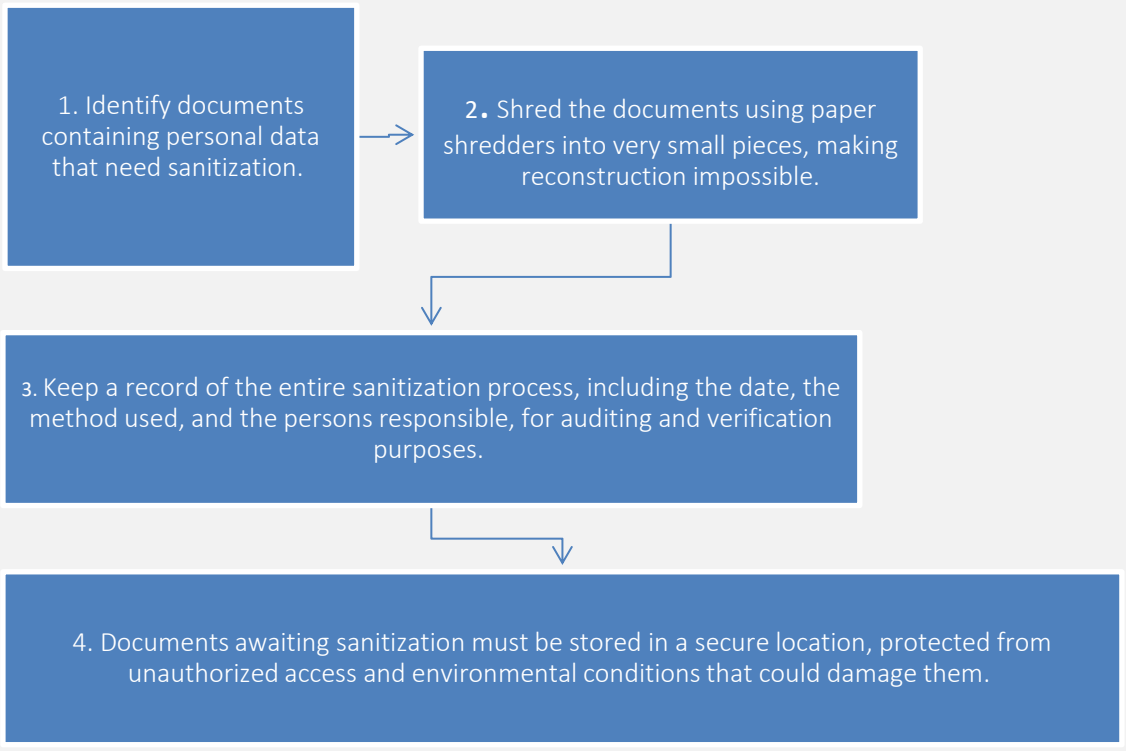
Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

11.1 Sanitization Routine – SBA

11.1.1 Sanitization of Physical Documents



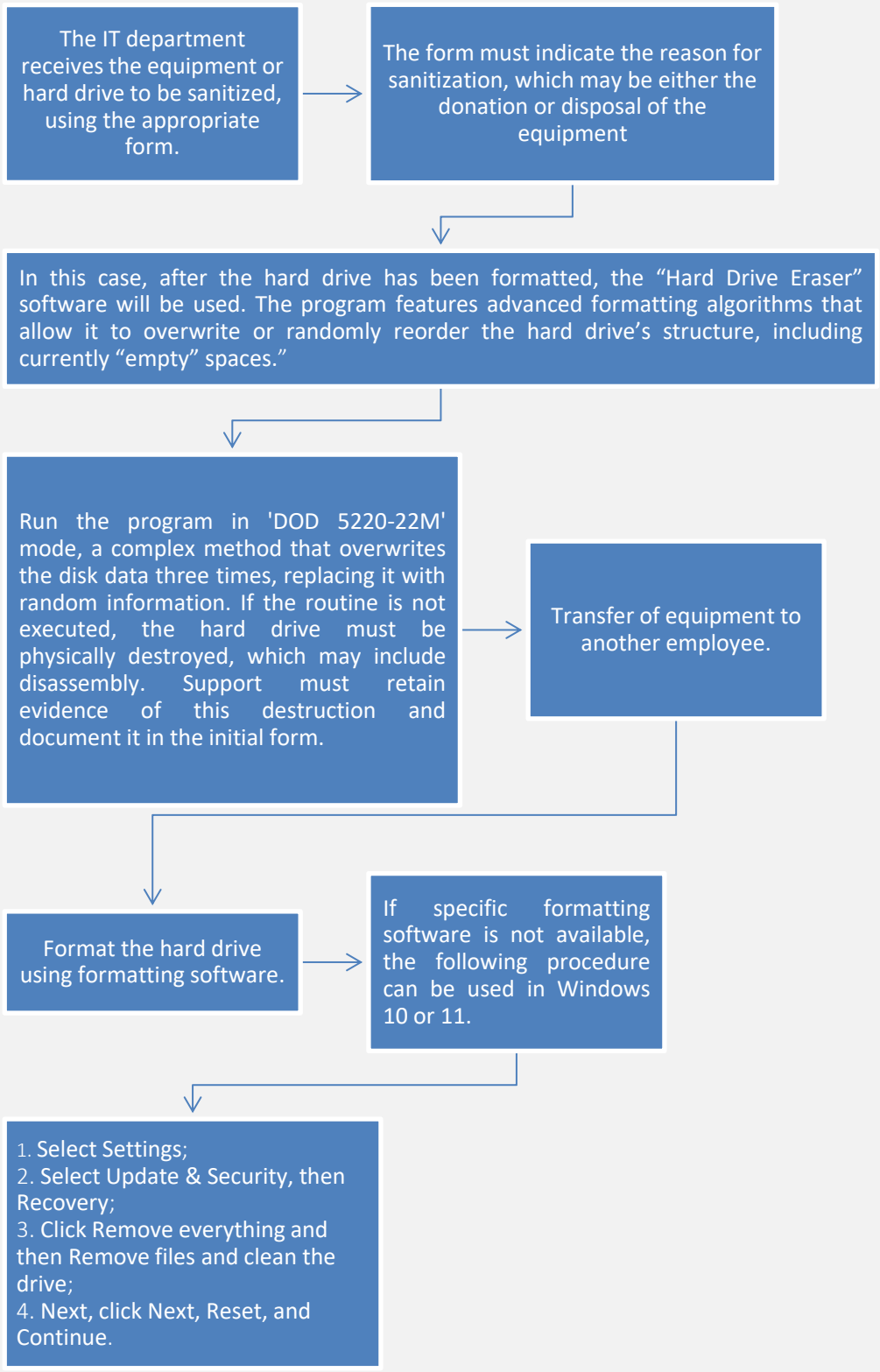
São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

11.1.2 Sanitization of Equipment



São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

12. Violations and Sanctions

The principles of this policy are fully endorsed by the Board of Partners of Santos Bevilaqua Advogados and are strictly followed by all members in the exercise of their activities. Under no circumstances will ignorance be accepted as an excuse for non-compliance with this policy and its derivatives.

12.1 Disciplinary Procedures and Violations

Santos Bevilaqua will establish formal disciplinary procedures for staff members, third parties, and service providers who commit infractions, violations, or serious security incidents. These infractions include non-compliance with the guidelines of this policy, as well as the Code of Ethics and Conduct Policy.

Violations of this policy include, but are not limited to:

- ⇒ Unauthorized use and disclosure of information, trade secrets, or other information without formal permission;
- ⇒ Illegal use of data, information, equipment, systems, and other technological resources, including violations of internal and external laws and regulations;
- ⇒ Any situation that exposes Santos Bevilaqua Advogados to financial losses or reputational damage due to breaches of confidentiality, or integrity, or availability of its information or information under its custody.
- ⇒

12.2 Sanctions and Responsibilities

All associates, third parties, and service providers must be aware that non-compliance with this policy will result in sanctions. These may be internal, administrative, legal, and/or criminal, depending on the severity of the violation.

For third parties and service providers, sanctions may include contract termination and civil or criminal liability to the fullest extent permitted by law.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

12.3 Violation Detection and Reporting

Upon detecting a violation, the user is responsible for immediately reporting it to the Information Security team. If it is found that an employee failed to report a known infraction, they may be considered an accomplice and subject to investigation and disciplinary action.

13. Validity and Review

This rule comes into effect on the date of its approval and shall be reviewed at a maximum interval of 12 months or whenever deemed necessary.

14. Version Control

Item	Date	Update	Responsible
v.1.0	11/5/2021	First version of the document	3A Plus Serviços de Informática Ltda
v.1.0	12/5/2021	Revision of the document	3A Plus Serviços de Informática Ltda
v.1.0	12/28/2021	Approval of the document	CSI - Santos Bevilaqua Advogados
v.2.0	12/5/2022	Revision	3A Plus Serviços de Informática Ltda
v.2.0	12/28/2022	Approval of the document	CSI - Santos Bevilaqua Advogados
v.3.0	12/5/2023	Revision	3A Plus Serviços de Informática Ltda
v.3.0	12/28/2023	Approval of the document	CSI - Santos Bevilaqua Advogados
v.4.0	2/1/2025	Revision	3A Plus Serviços de Informática Ltda
v.4.0	2/28/2025	Approval of the document	CSI - Santos Bevilaqua Advogados
v.5.0	7/9/2025	Revision	3A Plus Serviços de Informática Ltda
v.5.0	7/11/2025	Approval of the document	CSI - Santos Bevilaqua Advogados

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

15. Final Provisions

Just like ethics, security is a fundamental part of the internal culture at Santos Bevilaqua Advogados. Any security incident means someone has violated the firm's ethics and best practices.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar

CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro

Rua Lauro Muller, 116, sala 1903

CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br