Cryptography Guidelines

Santos Bevilaqua Advogados

Summary

1. Introduction

Santos Bevilaqua Advogados establishes information security rules with the objective of protecting its information assets against threats and minimizing risks and losses. We strive to ensure the availability of resources and maintain an effective security program, raising awareness among all staff members about the importance of data protection.

We recognize information as a critical asset, and its access is strictly managed to maintain confidentiality, integrity, and availability. Cryptography is an essential tool to mitigate interception and unauthorized access. It is applied to protect stored, processed, and transmitted data, as well as user credentials and secure communications.

This policy outlines Santos Bevilaqua Advogados' approach to cryptographic controls and management, defining the requirements and responsibilities necessary to achieve information security and data governance objectives. Encryption ensures that data remains unreadable to unauthorized parties, thus providing confidentiality, integrity, and authentication.

In accordance with the Brazilian Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados* – LGPD), which requires appropriate technical measures for the protection of data at rest and in transit, cryptography stands as a key solution. It is also vital for ensuring the integrity of data that, although publicly accessible, must be securely transmitted and stored.

Santos Bevilaqua Advogados is committed to continuously enhancing a corporate culture of information security, aligned with the acceptable use of information and its supporting assets, aiming to minimize risks and create a secure environment. This policy must be followed by all staff members, regardless of their level, role, or type of employment relationship.

2. Scope

This security policy covers all assets and environments of Santos Bevilaqua Advogados, whether physical or digital, where information is processed or stored.

Specifically, it applies to:

⇒ **Physical Environments:** Including office locations, data processing centers (DPCs), and any other property or premises under the custody of Santos Bevilaqua Advogados.

⇒ **Information Assets and Systems:** All IT resources and information processing systems that use encryption or require data protection under the custody of Santos Bevilaqua Advogados must comply with the terms of this policy.

⇒ **Personnel:** Applies to all staff members and service providers working with Santos Bevilaqua Advogados.

3. Objectives

Our information security policy aims to achieve the following essential objectives:

⇒ **Reduce risks:** Minimize information security risks to acceptable levels.

⇒ **Protect assets:** Ensure the confidentiality, integrity, and availability of the assets, services, and digital data of Santos Bevilaqua Advogados.

⇒ **Prevent losses:** Protect the firm’s information from theft or accidental loss on storage devices.

⇒ **Ensure secure transfers:** Ensure that the firm's information is protected during transfers between systems.

- **Strengthen cyber resilience:** Adopt the pillars of cyber resilience: Identify, Protect, Detect, Respond, and Recover.

- **Standardize encryption:** Define minimum standards and responsibilities for the encryption of digital assets.
- **Manage encryption consistently:** Ensure that encryption is managed in a uniform and appropriate manner.
- **Ensure data protection:** Provide data owners with the assurance that their information is protected.

4. Encryption Usage Guidelines

Santos Bevilaqua Advogados ensures the security of its information through a robust encryption system managed by the Information Security team.

This team is solely responsible for approving all encryption technologies and techniques used, as well as for the distribution and management of all encryption keys. It is essential that, even with encryption in place, authorized staff of Santos Bevilaqua Advogados have immediate access to the data, ensuring business continuity and enabling investigations. The team is also responsible for creating and publishing the encryption standards. These standards include, at a minimum, the type, strength, and quality of encryption algorithms required for different levels of protection, as well as complete key lifecycle management (generation, storage, retrieval, distribution, end of use, and destruction).

Information Security Team

All confidential information of Santos Bevilaqua Advogados must be encrypted in the following situations:

⇒ When transferred electronically or over public networks.

⇒ When stored on mobile devices (such as cell phones or laptops).

⇒ When at rest (stored on a server or system).

The encryption policy covers both data in transit (during transmission) and data at rest (stored on servers and systems). For the protection of data at rest, the measures may include:

⇒ Full disk encryption

⇒ Full file encryption

⇒ Full application encryption

⇒ Full database encryption

It is worth noting that all systems at Santos Bevilaqua Advogados use HTTPS certificates starting from authentication, to ensure secure connections.

Encryption implementation must always use approved methods and technologies. Standards, algorithms, protocols, and keys must comply with acceptable norms, and any unsupported ciphers, protocols, or algorithms should be disabled whenever possible.

Finally, cryptographic keys must be generated, stored, and managed securely to prevent loss, theft, or compromise. Access to keys must be performed using reliable and secure methods to maintain confidentiality and integrity. It is crucial that separate communication channels are used for the transfer of keys and data — they must never be transferred together over the same medium. Additionally, Santos Bevilaqua Advogados follows strict procedures and controls for the revocation of keys and certificates in case of compromise or expiration.

5. Keys

The encryption policy of Santos Bevilaqua Advogados structures the key lifecycle into four main phases:

⇒ **Pre-operational:** Keys are in the process of being created or activated and are not yet ready for use.

⇒ **Operational:** Keys are active and available for normal use.

⇒ **Post-operational:** Keys are no longer used regularly but may still be accessed in specific situation.

⇒ **Destruction:** Keys are permanently eliminated, along with all records of their existence.

6. Users

The encryption policy of Santos Bevilaqua Advogados ensures user identity verification. Only after authentication can the authenticated user's information be used within the system to define that user's authorizations. The use of cryptographic keys is only permitted after user identification. Therefore, to properly manage keys, the system must provide mechanisms for authentication and authorization or allow the use of keys within existing systems.

7. Implementation and Update

The Encryption Policy of Santos Bevilaqua Advogados shall be updated whenever necessary.