**americanas s.a.**

# INFORMATION SECURITY POLICY

## 1. Purpose

Providing principles, guidelines and regulations that comprise the Information Security Policy in order to ensure the safe processing of the Company's data information and communications.

## 2. Definitions

- **Assets**: Anything that has value for the Company.
- **Information assets**: Any and all resources that process, manipulate, store, transport, transmit and dispose of data and information having value to the Company and which require protection (for example: computers, servers, databases, smartphones, systems, environments and work processes, cabinets and files).
- **Authenticity**: Ensuring the identification of an individual responsible for a given action. Accordingly, the Company may ensure non-repudiation of the action performed, where and when it took place
- **Information life cycle**: The cycle existing from the creation or acquisition of information through use, manipulation, sharing, storage, transport and disposal thereof.
- **Information classification**: Process represented by the definition of a degree of confidentiality of the information and the groups of access thereto. It aims to ensure that information receives an adequate level of protection, according to its value, legal requirements, sensitivity and criticality for the organization.
- **Associate**: Employee, worker, intern, supplier, service provider, statutory or economic agent, who has access to information or resources of the Company.
- **Strategic Information Security Committee**: Group of individuals, at the Company, with the duty of acting as a forum for discussion, exchange of information and decision-making.
- **Confidentiality**: Status that information is not available or disclosed to unauthorized individuals, entities or processes.
- **Availability**: Status of being accessible and usable, on demand, by an authorized entity when required.
- **Document**: Set of information or instructions arranged in an orderly manner, which may be printed in hard copies or stored in electronic form. When stored in electronic form, it is also called "Digital Document".

- **Information security event**: Identified occurrence of a system, service or network, which evidences a possible violation of information security policy or failure of controls, or a previously unknown situation, which may be relevant to information security.
- **Document management**: Set of procedures and technical operations related to the production, processing, use, evaluation and archiving of documents in the current and intermediate stages, aiming at disposal or collection thereof for permanent storage.
- **Information security incident**: A single or a series of unwanted or unexpected information security events having a high probability of compromising business operations and threatening information security.
- **Information**: Set of interrelated data leading to the understanding of something and which bring a certain degree of knowledge. It may be provided in written, verbal or image form and stored in digital or physical medium. It is considered an asset that, like any other important asset, is critical for an organization's business and, accordingly, requires proper protection.
- **Integrity**: Assurance that the information is full and complete and that it has not been modified or destroyed in an unauthorized or accidental manner during its life cycle.
- **Classification level**: Category to be defined for each piece of information or class of information. Establishes the sensitivity of information in terms of preserving its confidentiality.
- **Personal data protection (privacy)**: Possibility for each associate or customer to autonomously determine the use that is made of their own personal data together with the establishment of assurances to prevent them from being used in a manner that causes discrimination or damages of any nature.
- **Information owner**: Individual responsible for ensuring that information and assets associated with information processing facilities are properly classified, performing from time to time critical reviews of classifications and access restrictions, taking into account applicable access control policies.
- **Information and communications security**: Ensuring preservation of confidentiality, availability, integrity and authenticity of existing information in any form or medium, such as printed, stored or transmitted by physical or electronic means, or even disclosed in audio visual media or spoken media in conversation.
- **Information processing**: Set of actions referring to the establishment of information protection guidelines according to the level of classification thereof, including: production, reception, use, access, reproduction, transport, transmission, distribution, destination, archiving, storage and disposal of Information.

- **Secure information processing**: Processing of information taking into account the criteria of Availability, Integrity, Confidentiality and Authenticity.
- **Company**: Comprises americanas s.a. and all other related companies, such as direct and indirect subsidiaries, and applies individually to any of the companies belonging to the same Economic Group.
- **User**: Any individual authorized to interact with the information. Access to the information shall be determined on a need-to-know basis for proper performance of the tasks inherent to their position or role.

## 3. Standard Contents

### 4.1. Roles & responsibilities

4.1.1. Strategic Information Security Committee (CESI)

The Company's Strategic Information Security Committee consists of executives from the Information Security area and Technology Officers, and may also use internal or external specialists for support in matters requiring specific technical knowledge.

4.1.1.1. CESI shall formally meet at least once every six months, and additional meetings shall be held whenever it is necessary to pass on resolutions on a serious incident or definition relevant to the Company.

CESI (Strategic Information Security Committee) shall:

4.1.1.2. Propose amendments to this document, review and validate the supplementary documents governing information security, promoting the continuous improvement of the Company's information security guidelines;

4.1.1.3. Propose information security-related investments aimed at reducing security risks and raising awareness among associates;

4.1.1.4. Decide on security incidents reported by the information security manager;

4.1.1.5. Provide support in the preparation of documents supplementary to this Policy with respect to classification, storage and maintenance of information;

4.1.1.6. Define the appropriate measures in the event of violation of this Policy;

4.1.1.7. Disseminate the Information Security culture in the Company;

4.1.1.8. Report to the Ame Committee formally, at least once a year, on the outcome of CESI meetings.

4.1.2. Ame Committee

The Ame Committee shall:

4.1.2.1. Monitor from time to time the performance and results of CESI;

4.1.2.2. Define the guidelines and propose improvements in the Information Security Policy;

4.1.2.3. Report from time to time to the Board of Directors any Information Security issues.

4.1.3. Board of Directors

The Board of Directors shall:

4.1.3.1. Approve the Company's Information Security Policy.

4.1.4. Executive and Statutory Board

The Executive Board shall:

4.1.4.1. Provide the human, material and financial resources necessary for the security of information and communications;

4.1.4.2. Monitor from time to time the evolution of information security indicators and results.

4.1.5. Information Security Manager

The Information Security Manager shall:

4.1.5.1. Report to the Executive Board for all aspects of security and risk management of the Company with respect to Information Security;

4.1.5.2. Respond for all information security events (physical or electronic) and all losses resulting from unmanaged or unanticipated risks;

4.1.5.3. Lead the preparation of the Corporate Information Security Policy, as well as the appendices necessary for the suitability of assets to the Security level relevant to the proper development of the business;

4.1.5.4. Pursue and support Information Security initiatives applicable to the entire Company, such as, for example, the security awareness program, information governance and digital identity management;

4.1.5.5. Ensure that security is part of the information planning process;

4.1.5.6. Support and validate external Information Security audits carried out by customers or regulatory agencies;

4.1.5.7. Liaison with relevant authorities, special interest groups or other specialized information security forums and professional associations;

4.1.5.8. Coordinate the work meetings of the technical/operational group in the handling of security incidents;

4.1.5.9. Evaluate information security incidents and propose corrective actions, including submitting them to the Strategic Information Security Committee, where applicable.

4.1.6. Area Manager

The Area Manager shall:

4.1.6.1. Ensure that the Company's Security Policy, regulations and procedures are in place and enforced in accordance with the provisions defined for its field of operation.

4.1.7. Associates

Associates shall:

4.1.7.1. Acknowledge and comply with the guidelines established in this Policy, as well as the good practices contributing to the security of information and communications at the Company;

4.1.7.2. Manage the resources, business processes and information under their responsibility in accordance with the guidelines under this Policy.

### 4.2. Information & communications security principles

Information & Communications Security actions at the Company are guided by the following principles:

4.2.1. **Strategic alignment**: alignment between the Company's Information & Communications Security Policy, regulations and actions with the Companies' mission and their strategic planning is mandatory.

4.2.2. **Organizational diversity**: the preparation of regulations, controls and the Company's Information & Communications Security Policy shall take into account the diversity of each Company's activities, respecting the nature and purpose of each Organizational Unit.

4.2.3. **Information ownership**: all information produced or stored at the Company is owned by the Company and not its Associates, Statutory Members and Service Providers, except in cases where the Company acts as custodian of the information, and use thereof shall be exclusively intended to meet the Company's interests.

### 4.3. Information & communications security guidelines

For the purposes of this Policy, the following general guidelines shall apply:

4.3.1. The Company's Information Security shall be supported by an Information & Communications Security Management System (ISMS).

4.3.2. Metrics and indicators allowing to control, audit and raise the Company's level of maturity and compliance with respect to information security shall be defined.

4.3.3. Commitment: All Associates, Statutory Members and Service Providers of the Company, in any relationship, role or hierarchical level, are responsible for protecting and safeguarding the technological assets and information of which they are users, the physical and computing environments to which they have access, observing the Policies and mechanisms of control and protection put in place.

4.3.4. Risk Management: All processes, products and services developed, which may compromise information security, shall be submitted to a formal process of review, assessment and treatment of risks, before acquisition, implementation and availability thereof in order to reach the degree of security appropriate for the Company.

4.3.5. Business Continuity Management: the Company shall establish a set of documented, tested and regularly revised strategies and action plans in order to ensure that its essential services are properly identified, preserved and delivered, even in the event of a disaster until the Company's regular operating situation is resumed.

4.3.6. Information Classification & Processing: All information and the respective technological resources supporting such information shall be classified according to their degree of confidentiality and properly processed to ensure protection thereof throughout their life cycle.

4.3.7. Access Management: Access to the Company's physical and logical environments shall be controlled, recorded and monitored, based on the principles of need-to-know and least privilege for the performance of professional activities.

4.3.8. Incident Management: The Company's Associates, Statutory Members and Service Providers are required to immediately report any security incidents that they become aware of so that such incidents may be recorded, evaluated and treated.

4.3.9. Audit & Compliance: The Company reserves the right to audit from time to time the information and communications security practice in order to assess the compliance of the actions of its Associates and Service Providers in relation to the provisions of the Information & Communications Security Policy of the Company and applicable law.

4.3.10. Monitoring: The Company reserves the right to monitor access and use of its physical environments, as well as technological environments, equipment and systems, so that undesirable or unauthorized actions are proactively detected.

4.3.11. Training & Awareness: All Associates, Service Providers and Statutory Members shall acknowledge this Policy and be trained on an annual basis through awareness campaigns and training in accordance with their duties. They shall be aware of this Policy and sign the respective acceptance term, thus ensuring greater effectiveness and efficiency of information security actions at the Company.

4.3.12. Management of exceptions/scheduling procedures: The valid needs of the Company arising from its operations may eventually conflict with guidelines established in this Policy. Exception management procedures recognize that Policy conflicts are natural and that the Company is mature enough to be able to manage them. By establishing exception management procedures, associates are encouraged to work with the system rather than work around it. Area managers shall be consulted about omissions so that new procedures may be established to adjust to exceptions.

4.3.13. Change Management: Change Management shall ensure that methods and procedures are properly applied to evaluate, approve, implement and review all Changes within the established scope effectively in order to minimize risk and potential impact of such Changes on the business. The processes and controls established shall allow the traceability of changes occurring in the Company's critical environments.

4.3.14. Secure Development: Applications developed or acquired by the Company shall employ methodologies ensuring information security throughout the system development cycle.

### 4.4. Privacy

4.4.1. The Company respects the privacy of the personal data of its associates and customers.

4.4.2. In terms of privacy protection, only data necessary for the purpose or legally required for the Company's effective performance and compliance with legal obligations are requested and retained or eventually disclosed in compliance with specific law.

4.4.3. The Company reserves the right to monitor the use of computers, landlines, smartphones, tablets, mobile phones, radios and other available equipment and network activities, including, but not limited to, email, voicemail, Internet usage and any information stored on such equipment, systems or servers, in appropriate circumstances and with a view to protecting information and the security of information and content traffic.

### 4.5. Critical approvals, reviews & analyzes

4.5.1. The set of documents comprising the Company's Information & Communications Security Policy shall undergo annual reviews and critical analysis from time to time or whenever a relevant fact or event occurs requiring an early review.

4.6. **Violations of corporate information security policy**

4.6.1. In the event of violation of this Policy, please notify the Information Security immediately and, ultimately, the Strategic Information Security Committee.

4.6.2. Failure to comply with the guidelines provided for in this Policy is subject to administrative sanctions, according to the internal regulations of the Human Resources area, and legal sanctions, according to applicable law.

4.6.3. Note: Failure by the associate to comply with the established guidelines and rules (Company's Security Policies & Regulations), whether individually or cumulatively, may give rise to penalties, according to the violation committed.

## 4. References

- ABNT NBR ISO/IEC 27001:2013
- ABNT NBR ISO/IEC 27002:2013
- CCS CSC 16
- COBIT 5
- ISA 62443-2-1:2009 & ISA 62443-3-3:2013
- NIST SP 800-53 Rev. 4
- Code of Ethics and Conduct
- LGPD (General Personal Data Protection Law, Law No. 13.709/2018)
- PCI DSS

## 5. Appendices

### 6.1. Term of Individual Acknowledgment of Commitment & Confidentiality

- AMER-TER-SI-01 - Term - Information Security

### 6.2. Information Security Regulations:

- AMER-REG-SI-001 Internet Access
- AMER-REG-SI-002 Information Classification & Processing
- AMER-REG-SI-003 Access Control
- AMER-REG-SI-004 Secure Development
- AMER-REG-SI-005 IS Incident Management

- AMER-REG-SI-006 Risk Management
- AMER-REG-SI-007 Mobile Device Usage
- AMER-REG-SI-008 E-Mail Usage
- AMER-REG-SI-009 IS Internal Audits
- AMER-REG-SI-010 Change Management

## 6. TERM

This Policy comes into force on the date of publication thereof.