INFORMATION SECURITY POLICY

ambipar GROUP

I. PRESENTATION

Ambipar works in many different sectors to offer services and products that are focused on environmental management. In a full global expansion, Ambipar follows compliance and environmental responsibility guidelines, maintaining ethical standards and promptly meeting clients' demands.

Therefore, the Information Security Policy, also referred to as ISP, is a document that guides and establishes Ambipar's corporate guidelines to protect information assets and to prevent legal liability for all users.

Thus, it must be followed and implemented in all areas of the company.

The current ISP is based on the recommendations proposed by the ABNT NBR ISO/IEC 27002:2005 standard, known globally as a code of practice for information security management, and is in accordance with the applicable laws in our country.

1. PURPOSE

The objective of this document is to ensure the confidentiality, integrity, availability, legality, authenticity, and auditability of the information of the organization and of every person who is a part of it, such as clients, suppliers, employees, and shareholders.

2. SCOPE OF APPLICATION

The document applies to all administrators, employees, interns, service providers, systems, and services, including services performed externally or by third parties that may use the processing environment or have access to information owned by Ambipar or its subsidiaries.

Every single person who may use the company's computing resources is responsible for protecting the safety and integrity of the information and the IT equipment.

3. CONCEPTS

Information security is hereby characterized by the preservation of the following concepts:

- Confidentiality: Ensures that information can only be accessed by authorized personnel for the necessary amount of time;
- Availability: Ensures that information is available to the authorized personnel when needed;
- Integrity: Ensures that information is complete and true, and that it is not modified or destroyed without permission or accidentally during its lifecycle.

4. DEFINITIONS

Information: The result of a system's record or data (physical or electronic) processing and organization.

Information Assets: Set of information, stored in such a way that it can be identified and recognized as valuable to the company.

Information Systems: Generally, these are computing systems used by the company to support its operations.

Segregation of Duties: Consists in breaking down roles into separate functions – authorization, approval of operations, execution, control, and accountability, in such a way that no employee, intern, or service provider may hold powers or duties that are not in accordance with this principle.

Information Technology Manager: Ambipar's IT department, which aims to assess the information security strategy and guidelines followed by the company.

5. INFORMATION CLASSIFICATION

All information created during the development of the company's activities must be classified according to the levels of confidentiality below:

1. Public: Information that may be accessed by the organization's users, clients, suppliers, service providers, and the general public. For example: information available on Ambipar's webpage.

2. Internal: Information that may only be accessed by the organization's employees. This involves information with a level of confidentiality that may harm the image of the company. Example: HR notice intended for employees.

3. Confidential: Information that may be accessed by the organization's users and partners who are specifically authorized to do so. Unauthorized disclosure of this type of information may have an impact – financially, to the image or operations – on the company's or the partner's business. Example: Business proposals.

4. Restricted: Information that may only be accessed by the organization's users who are explicitly specified by name or the department they work in. Unauthorized disclosure of this type of information may lead to serious damage to the business and/or jeopardize the organization's business strategy. Example: Access to payroll information is restricted to the HR department only.

6. RESPONSIBILITIES

Generally, all administrators, employees, interns, and service providers are responsible for:

- Faithfully complying with Ambipar's Information Security Policy;
- Protecting information against access, modification, destruction, or disclosure that has not been authorized by Ambipar;
- Ensuring that technology resources, information, and systems at your disposal are used only for the purposes approved by Ambipar;
- Not using Ambipar's technology resources in public networks without the proper safety protocols (e.g., public wireless networks in airports, coffeeshops, etc.);
- Following the laws and standards governing intellectual property;

- Not discussing confidential work-related matters in public environments or open spaces (airplanes, transportation, restaurants, social meetings, etc.), including posting comments and opinions on blogs and social media;
- Not sharing confidential information of any kind;
- Immediately communicating any non-compliance issues or breach of this Policy and/or its Standards and Procedures to the IT department.

At Ambipar, it is everyone's responsibility:

To consider the information as the organization's asset, a critical resource to carry out its business activities, which holds great value to Ambipar and must always be treated in a professional manner.

It is the responsibility of the Director/Superintendent/Manager/Coordinator/Supervisor of each department to classify the information (reports, documents, models, procedures, spreadsheets) generated by their department according to the level of confidentiality set forth in this document.

Best practices include:

Blocking access to the computer any time you leave your desk, even if only for a few minutes;

Keeping desks organized and locking documents that contain confidential information when you are not using them.

II. GENERAL GUIDELINES

1. Employees' Personal Data

Ambipar is committed not to accumulate employees' personal data beyond the data relevant to conducting its business. All personal data belonging to employees will be considered confidential.

Employees' personal data under the responsibility of Ambipar will not be used for any intentions other than the purposes they were collected for.

Employees' personal data will not be transferred to third parties, except when required by our business and as long as the third parties are able to maintain the confidentiality of said data.

2. Hiring/Firing Employees

Ambipar's HR department shall inform the Information Technology Manager of any movements involving employees, contingent workers and/or interns, as well as if any employee has been hired/fired, so that they can be registered in or removed from the company's systems. HR must ask the department in charge of hiring about which systems and file repositories the new employee will have access to.

This information will be registered and forwarded to the Information Technology Manager through the "RH.003 – Granting / Suspension of Access" authorization. Then, Ambipar's Information Technology Manager will register and inform the new user of their first password, which must be changed by the user at the time of their first access.

In case an employee is fired, the HR department must communicate the event on the same day to the Information Technology Manager through the "RH.003 – Granting / Suspension of Access" authorization, so that any access granted may be revoked.

It is up to the HR department to inform and obtain the proper signatures to confirm the new hires agree to following Ambipar's Information Security Policy.

3. Password Policy

Passwords to access the systems used by/at the company, which are provided by Ambipar's Information Technology Manager, are for personal use and are non-transferable. It is EXPLICITLY forbidden to share passwords with other users, and doing so will be considered a serious contractual infringement.

Access and data/activities generated through login and password credentials provided by Ambipar's Information Technology Manager are the user's responsibility.

The passwords set up for access must meet the following recommended complexity requirements to be accepted by the system-specific policies:

- Passwords cannot contain the user account name, user's name, or any part of it;
- Passwords must contain characters of the following categories: - Upper case letters - Lower case letters - Base-10 numerals (0 to 9) - Non-alphanumeric characters (special characters): (~!@#$%^&*- +='|\() {} []:;'" <>,.? /);
- Passwords will expire every 90 days, and it is mandatory to change it at the end of this period, following the requirements set out above, without repeating any of the last 5 passwords;
- The first passwords created must be random, as recommended by the best practices, without following patterns that may be easily detected or using the same standard password for all Ambipar's users, which would put their safety at risk;
- The first passwords of domain users must be changed during their first access to the Ambipar network. If equipment is not in the company's domain, this change must be made via VPN. For other systems, the password must be changed as per usual in the system.

Any time an employee is fired from the organization, all passwords and access are revoked on the same day.

4. Work Files

Work files, which are considered critical data for the development of the business, are kept in Ambipar's file servers.

Examples of work files include:

- Revenue worksheet;
- Invoices;
- Business proposals;
- Technical analysis reports;
- Measurement worksheets;
- System documentation used as input for the analysis and measurement work.

Access to the file server outside Ambipar's facilities will be blocked and is forbidden, except when accessed through VPN with proper authorization from the Information Technology Manager.

5. Individual Files

Individual files are files that have been created, copied, or developed by users, but are not part of the deliverables of their work, whether internal or for customers. A few examples include drafts or reminders, calculation reports, messages, diagrams, or technical instruction. It is the responsibility of the users to back up these files.

Users are not allowed to use or store the following types of related files in their workstations:

- Programs that are not licensed or certified for use at Ambipar;
- Music, movies, TV shows;
- Videos not related to professional activity;
- Pornographic or sex-related content.

If there is a need to share data among users (internal and/or external), the file server or corporate email provided by Ambipar must be used, with the consent from the Manager in charge.

6. Sharing Folders and Data

Sharing work files and folders that may contain information classified as CONFIDENTIAL or RESTRICTED is prohibited through the following channels:

- Google Talk, WhatsApp, Viber, or any other instant messaging tool;
- File sharing on Windows;

- Bluetooth;
- Copies on flash drives or any other removable device;
- Google Drive, Dropbox, iCloud, OneDrive, or any other virtual drive.

7. Backup Copies, Recovery, and Integrity of the Systems and its Databases

Backup copies of the systems, repositories in the work file network, databases, and equipment and network server configurations are the sole responsibility of the Information Technology Manager.

8. Internet Use

Internet use will be monitored by the Information Technology Manager through the browser recording system, which discloses which user is connected, how long they used the Internet for, and what pages they accessed.

Employees who will be allowed to use (browse) restricted websites, such as social media, will be assigned by the company's management through a request from their Director/Superintendent/Manager/Coordinator/Supervisor.

Users must make sure they are not taking actions that may infringe on third party copyright, trademarks, use licenses, or patents.

When browsing the web, viewing, transferring (downloading), copying, or any other type of access to these websites are forbidden:

- Radio stations;
- Online games;
- Pornographic or sex-related content;
- Websites promoting illegal activities;
- Websites promoting contempt for or denigration or incitement of certain groups;

Websites that promote participation in chat rooms on matters related to FATO's business, that do not contain information that adds professional and/or business knowledge should not be accessed.

Any access to social media that does not pertain to the area of interest of the company is not permitted, and therefore, is subject to penalties.

In cases where there may be a need to access a certain blocked website or port, an "TI.002 – Infrastructure (Level 1 Support / Network and Internet / Servers)" authorization must be requested, with the website URL and/or port number, so that the Information Technology Manager can provide clearance with Ambipar's firewall.

9. Use of Electronic Mail ("email")

The electronic mail provided by Ambipar is an internal and external communication instrument for conducting the company's business.

Messages must be stated in a professional manner, must not harm Ambipar's image, and must not be contradictory to the applicable law or the ethical principles set out in the "Code of Ethics and Conduct."

The electronic mail is a tool used to send and receive messages instantly via the Internet, and users are responsible for all messages sent from their email address.

Registering personal contact information in the instant messaging systems is forbidden (when using the corporate address @ambipar.com), as is using personal accounts.

Using Microsoft's multifactor authentication is mandatory, and users are also required to use Microsoft Authenticator passwords to use apps that are not browsers with the corporate email. For browsers, the user can provide other types of authentications, in addition to the authenticator app password, such as sending a text message or via phone call for personal or corporate phones, since the user's email password is strictly for personal use.

It is strictly forbidden to send messages:

- That contain defamatory statements and offensive language;
- That may cause harm to others;
- That are hostile;
- That are related to "chain messages", to pornographic content or similar;
- That may harm Ambipar's image, its subsidiaries, and/or other companies;
- That are not in accordance with the policies set out in Ambipar's "Code of Ethics and Conduct";
- Through free email accounts (Yahoo!, Hotmail, etc.) on Ambipar's computers.

It is important that users are careful when opening an email from an unknown sender, especially if this email is redirected to a link and/or if there are any attachment files. For greater safety in case of a suspicious email, it must be forwarded to spam@ambipar.com, where the Information Technology Manager will conduct a more thorough analysis and determine whether it will be blocked or disclosed.

To prevent viruses or any other malware on Ambipar's computers, the Information Technology Manager may block emails sent from free accounts.

10. Need for New Systems, Apps, and/or Equipment

The Information Technology Manager is responsible for determining purchases, replacements, and installation of any "software" and "hardware."

Software and hardware can only be acquired by opening a ticket in the Workflow system (the "TI.012 – Acquisition of Electronic Equipment" authorization for acquiring software licenses and equipment, or the "TI.002 – Infrastructure [Level 1 Support / Network and Internet / Servers]" authorization for installing licensed software), with the attached authorization from the requesting user's director. Purchasing or developing software directly by the users is not permitted.

Equipment can only be delivered after a statement of liability, intended for the employee responsible for the equipment, is signed by opening a ticket on Workflow of the "TI.019 – Statement of Liability for Electronic Equipment" category.

11. Use of Company-Owned Equipment

The use of personal equipment (laptops/desktops) is forbidden for the performance of duties, and the Company will provide equipment that is compatible with the activities performed by the employee / partner, when necessary, except when expressly authorized by the Senior Management, upon formal request from the party.

It is the responsibility of Ambipar's Information Technology Manager to install software and hardware, following maintenance, licensing, and acquisition agreements and terms celebrated by Ambipar.

The user is not authorized to install software, including those made available on the Internet (even if it is free, such as freeware/shareware), or new hardware components on Ambipar's equipment, even if they are intended for or facilitate the user's professional activities.

It is the responsibility of the Information Technology Manager to maintain any infrastructure equipment. Third-party vendors may only perform maintenance work with the Information Technology Manager's approval and a budget previously approved by the board.

It is the user's responsibility to allow access to their equipment for use by employees authorized by the Information Technology Manager, in order to perform maintenance and inspection work (including remotely), on a date and time previously scheduled. The Information Technology Manager is responsible for deleting potential files, software, or hardware installed / saved on the equipment that are not in accordance with the current Policy, without the need for any previous notices / consent.

Users who are in possession of any equipment (desktop, laptop, cellphone, tablet or other information technology equipment) owned by Ambipar must be aware that:

- Information technology resources are made available to the users for the purpose of performing professional activities;
- Protecting the computing resource of individual use is the responsibility of the user;
- It is the responsibility of the user to ensure the integrity of the equipment, as well as the confidentiality and the availability of the information on it;
- The user must not change the configuration of the equipment received;

- The user must not install or remove any programs on the equipment, nor can they change the configuration of any previously installed programs.

Removable media (USB drives, cards, CDs, DVDs) can only be used with the previous authorization by the user's direct manager and must be approved only by the Information Technology Manager upon express approval, as mentioned.

Outside of the Workplace:

- Keep the equipment with you at all times;
- Pay attention in hotel lobbies, airports, airplanes, bus, taxi, etc.
- When transporting the equipment in a vehicle, always place it in the trunk or somewhere it is not visible;
- Pay attention when carrying the equipment around on the street.

In Case of Theft:

- File a report at the police station;
- Disclose the incident as quickly as possible to your immediate superior and to the Information Technology Manager;
- Send a copy of the police report to HR.

12. Data

All data (files, documents, presentations, etc.) must be mandatorily stored in the file server specified by Ambipar ("network") for the protection, maintenance, and confidentiality of this information, as data stored locally on the computer is not protected by regular backups and, in case there are any problems with the equipment, may result in partial or total loss of Company's key data.

Failure to follow this guideline may characterize contractual infringement, as it goes against the information security best practices.

Only data pertaining to the company may be stored on Ambipar's computers.

It is the responsibility of the Information Technology Manager to ensure that regular backups are routinely performed in all Ambipar's servers, so as to prevent against data loss.

13. Printing

The user must ensure that, after printing out any documents with confidential information, they are not exposed to others who may use the shared printer. The user must also ensure the proper disposal of said documents.

With the purpose of enabling information security, most of Ambipar's printers have a system in place to allow only the user to have access to the printouts through a PIN or their badge.

14. Telecommunications System

Controlling the use of and granting access and applying restrictions to Ambipar's phone extensions, as well as the use of potential virtual extensions installed on the computers, are the responsibilities of the Information Technology Manager, according to the specifications set by the company's management.

15. Use of Antivirus Software

Every file obtained via the Internet or received from an external entity to Ambipar must be verified by an antivirus software.

All workstations have an antivirus software installed on them, and updates are automatic, through the network, scheduled by the Information Technology Manager.

The user may not, under any circumstances, disable the antivirus software that is installed in the workstations.

III. RESPONSIBILITIES OF THE DIRECTORS / SUPERINTENDENTS / MANAGERS / COORDINATORS / SUPERVISORS

Directors, superintendents, managers, coordinators, and supervisors are responsible for defining their subordinates' access rights to the company's systems and information. It is up to them to confirm if employees are correctly accessing the systems and data areas compatible with their respective duties, as well as properly using and maintaining the equipment and keeping backup copies of their individual files, as established in this policy.

The Information Technology Manager will conduct regular audits of the users' access to the information to confirm:

- What type of information the user can access;
- Who is authorized to access a specific system and/or information;
- Who accessed a specific system and information;
- Who authorized the user to access a specific system or information;
- What information or system a specific user accessed;
- Who tried to access any system or information without the proper authorization.

IV. BREACH OF THE SECURITY POLICY

A breach is any action that:

- Exposes the company to an effective or a potential monetary loss by jeopardizing the data or information security, or the loss of equipment;
- Involves the disclosure of confidential data, copyrights, negotiations, patents, or unauthorized use of corporate data;

- Involves the use of data for illegal purposes that may include the violation of any law, regulations, or any other government devices.

V. OTHER

Any other IT-related subjects that have not been addressed in this document must be communicated to the Information Technology Manager so that further instructions can be provided.

VI. PENALTIES

Failure to comply with this Information Security Policy will imply serious infringement and may result in the following measures:

- Formal warning;
- Suspension;
- Termination of employment contract;
- Other disciplinary action and/or civil or criminal proceeding.

VII. DURATION

The provisions in this document will come into effect on the date the release is published for the announcement, as approved by the Executive Board.