



Summary

1. INTEGRATED MANAGEMENT SYSTEM – IMS (SGI)	3
1.1 INTRODUCTION	3
1.2 SCOPE	4
1.3 GUIDELINE	5
2. MICROWARE POLICIES	6
2.1 INFORMATION SECURITY	6
2.1.1 DATA PROTECTION	6
2.1.1.1 DEFINITION OF PERSONAL DATA	9
2.1.1.2 DUTY OF INCIDENT AND CHANGE REPORTING	9
2.1.2 CONFIDENTIALITY POLICY	9
2.1.2.1 PRIVILEGED INFORMATION	10
2.1.2.2 SECRECY AND CONFIDENTIALITY	10
2.2 GOVERNANCE AND ANTI-CORRUPTION	11
2.2.1 ANTI-CORRUPTION POLICY	11
2.2.1.1 OBJECTIVE AND SCOPE.....	11
2.2.1.2 GENERAL CONSIDERATIONS ABOUT ANTI-CORRUPTION LAW ..	11
2.2.1.3 CONDUCTS PROHIBITED BY THE ANTICORRUPTION LAW.	11
2.2.1.4 RESPONSIBILITY OF ALL EMPLOYEES	12
2.2.1.5 RESPONSIBILITY OF ALL STAKEHOLDERS	12
2.2.1.6 EXAMPLES OF SITUATIONS OF ATTENTION.....	13
2.2.1.7 CULTURE AND AWARENESS	13
2.2.2 CODE OF ETHICAL CONDUCT	14
2.2.2.1 WORK ENVIRONMENT	14
2.2.2.2 BIDS, PURCHASES AND CONTRACTS	15
2.2.2.2.1 SPECIFIC SITUATIONS.....	15
2.2.2.2.2 SPONSORSHIP	16
2.2.2.2.3 GIFTS AND HOSPITALITIES	16
2.2.3 MONITORING COMPLIANCE WITH GOVERNANCE POLICIES	17
2.2.3.1 COMMUNICATION CHANNEL	18
2.3 IT SERVICES MANAGEMENT	18





2.3.1 STANDARD SERVICE LEVEL	18
2.4 SUSTAINABILITY POLICY	19
3. TERM OF AGREEMENT	20

1.0 - INTEGRATED MANAGEMENT SYSTEM

1.1 - Introduction

Microware has implemented an Integrated Management System, in the units of São Paulo and Rio de Janeiro, guided by the norms below, for better execution of its processes, safely and with excellent IT services:

NBR ISO 9001:2015: Process and Quality Management certified since 2008 - In Microware's 4 units: RJ, SP, ES and DF.

ISO/IEC 20000-1:2018: IT Service Management since 2022 - In Microware's RJ and SP units.

NBR ISO/IEC 27001:2013: Information Security Management since 2022 - At Microware units in RJ and SP.

Certigov: Compliance and Business Ethics certified since 2018 - At Microware's ES unit.





1.2 - SCOPE:

NBR ISO 9001:2015:

Commercialization of Information Technology Products and Systems and Provision of Services Information Technology Consulting, Installation, Configuration, Maintenance, Support and Allocation of Professionals, Systems and Equipment.

ISO/IEC 20000-1:2018:

IT Service Management System that supports the delivery of IT services to clients, from Microwave's facilities in São Paulo and Rio de Janeiro, according to the catalog of including installation, configuration, maintenance and support services for equipment and systems.

NBR ISO/IEC 27001:2013:

Microwave's Information Security Management System for the Commercialization of Information Technology Products and Systems and the Provision of Information Technology Services of Advice, Installation, Configuration, Maintenance, Support and Allocation of Systems and Equipment, according to the declaration of applicability in its version 11 of 13/09/2024.

CertiGov:

MICROWARE's Management System to ensure compliance and to combat corruption and bribery, in any of its forms, in the public and private spheres, in the Commercialization of Information Technology Products and Systems and in the Provision of Information Technology Advisory Services, Installation, Configuration, Maintenance, Support and Allocation of Professionals, Systems and Equipment.





1.3 - GUIDELINE:

To be Reference:

- In the Marketing of Information Technology Products and Systems.
 - In the Quality of our Processes.
 - In the rendering of services in Information Technology of Consultancy, Installation, Configuration, Maintenance, Support and Allocation of Professionals, Systems and Equipment.
 - Confidentiality, Integrity and Availability through Information Security Management.
- Security Management.

Offering objective solutions in IT, to meet the needs of our clients, based on training and qualification of employees, continuous improvement of its management system and meeting the standards and legislation in force.





2.0 - MICROWARE POLICIES

2.1 - INFORMATION SECURITY

2.1.1 - DATA PROTECTION

The Parties, by mutual agreement, agree to comply with the duties and obligations regarding the protection of Personal Data and undertake to treat the Personal Data collected under the Agreement, if any, in accordance with the applicable legislation in force, including, but not limited to Law No. 13,709, dated August 14, 2018 ("General Data Protection Law" or "LGPD"), and in accordance with the Marco Civil da Internet Law No. 12,965 and Decree 8,771/2016, to the extent applicable. The Parties shall also ensure that their employees, agents and subcontractors observe the provisions of the legal diplomas in reference related to the protection of personal data, including, but not limited to, the LGPD.

Each Party shall ensure that any Personal Data it provides to the other Party has been collected in compliance with applicable law as well as has a legal relationship with the data subject of the Personal Data. The Parties shall take the necessary measures, including providing adequate information to the Personal Data Subjects and ensuring that a legal basis exists a legal basis, so that the other Party is entitled to receive such Personal Data for the purposes of this Agreement. The Party providing the Personal Data shall be responsible for the safe transmission of such Personal Data to the other Party.

The Party receiving the Personal Data provided by the other Party shall treat the Personal Data only Personal Data only to the extent necessary to achieve the purpose for which the Personal Data were provided and to fulfill its obligations under the Agreement. The Parties acknowledge that Personal Data shall be processed if necessary to comply with a legal or regulatory legal or regulatory obligation to which the Party is subject in Brazil or for the exercise of rights in judicial, administrative and arbitral proceedings

The Parties acknowledge that, for the purposes of administrative management and fulfillment of the obligations the Agreement, both need to receive and process all Personal Data mentioned in the mentioned in the Agreement or in the other ocuments that regulate the relationship between them and/or the owners of the Personal Data, as well as any others that may be necessary in the event that concrete. The Parties shall not be liable for any damages caused by the processing of

outdated, inaccurate or otherwise incorrect Personal Data that they have received from third parties.





Personal Data will be handled under the terms of the Agreement, the applicable legislation and the other policies and documents applicable to the contractual relationship existing between the Parties. The purposes for which processing of Personal Data are limited to the scope of the Agreement.

The Parties declare that the Personal Data processed by them will not be shared with third parties who have no relation with the fulfillment of the obligations established in the Agreement, except in the event of a judicial request, regulatory force or law and express authorization of the Personal Data, and such third parties will handle the Personal Data exclusively for the purposes solely for the purposes permitted by the Party controlling the Personal Data, including for those described in clause 2.3.1.

If either Party receives a complaint, inquiry or request from a data subject personal data with regard to the processing of Personal Data (including, without limitation, any request for access, rectification, deletion, portability, revocation or restriction of processing of personal data) in accordance with Article 18 of the LGPD and, if the assistance of the other Party is necessary to respond to the complaint, inquiry and/or request, that Party shall notify the other Party other Party within five (5) business days. In such case, the notified Party shall cooperate with the notifying Party.

Each Party shall be individually responsible for compliance with its obligations under of the LGPD and any regulations issued thereafter by competent regulatory authority. competent regulatory authority.

Each Party undertakes to keep Personal Data confidential, adopting technical and measures to protect Personal Data against unauthorized access and accidental or unlawful destruction, loss, alteration, communication or disclosure ("Unauthorized or Incidental Processing or Incident").

The Parties, including all of their employees, undertake to treat all Personal Data as Personal Data as confidential and in line with the provisions set out in the confidentiality confidentiality clause of the Agreement, unless already known to the public, even if the Agreement is terminated and regardless of the reasons for its termination.

Each Party shall notify the other Party in writing within seventy-two (72) hours of any Unauthorized Treatment or Incident or breach of the provisions of this Section, or if any notification, complaint, inquiry or request is made by a regulatory authority due to the





processing of Personal Data in connection with this Agreement. Such notice shall contain at least: (i) a description of the nature of the Personal Data affected; (ii) information (iii) information about the technical and security measures used for the protection of personal data (iv) the risks related to the incident; (v) the reasons for the delay, in case delay, in case the communication was not immediate; and (vi) the measures that have been or will be adopted to reverse or mitigate the effects of the damage caused.

Each Party undertakes to keep Personal Data confidential, adopting technical and measures to protect Personal Data against unauthorized access and accidental or unlawful destruction, loss, alteration, communication or disclosure ("Unauthorized or Incidental Authorized Treatment or Incident").

In case the contractor has access to the database of systems provided by it, which exist service or other applications by virtue of the service provided, it must not, under any circumstances, allow the access to the database of the systems provided by it. under no circumstances allow its employees access to the contents of this database.

Each Party shall be liable to the other Party ("Aggrieved Party") for any damages caused as a result of (i) the breach of its obligations under this Agreement or (ii) the violation of any rights of the owners of personal data and including, but not limited to the (iii) misuse of the Personal Data obtained through the Agreement and shall indemnify the Injured Party for any and all expenses, costs, expenses, attorneys' fees and procedural incurred or compensation/fines paid as a result of such violation.

For the purposes of this Section, in the event that the Bereaved Party receives any claim that is to be indemnified by the other Party, it shall: (i) notify the responsible Party pursuant to (ii) grant the responsible Party exclusive control over the claim; (iii) refrain from any act or (iii) refrain from doing any act or signing any agreement, without the prior consent of the responsible Party.

The responsible Party may choose legal counsel of its own discretion and shall bear all costs, expenses and fees for the defense of the Defendant Party, without prejudice to the Injured Party, at its own discretion and expense, may hire its own counsel.

Without prejudice to any joint cooperation in case of fulfillment of the rights of the holders and notification of Unauthorized Processing or Incident, the Parties shall be liable to the competent authorities for their own acts and omissions that gave rise to the non-compliance with applicable laws and regulations.





2.1.1.1 - DEFINITION OF PERSONAL DATA

Under the terms of the General Data Protection Law, Personal Data is understood to be any information related to an identified or identifiable natural person that is collected as a result of the obligations obligations contractually assumed by the Parties, as well as information that is shared or made shared or made available between the Parties under the Contract (simply "Personal Data").

2.1.1.2 - DUTY TO REPORT INCIDENTS AND CHANGE

The Party shall report to Microware, as soon as possible, the occurrence of any security incident related to the processing of personal data object of this contract, under penalty of a daily fine.

The Party shall notify Microware of any change that may impact a process, a service or the service or Information security, so that the change is planned together with Microware.

Communication must occur via e-mail to seguranca.grupo@microware.com.br and/or on the Security Incident or Security Risk Report Form available on our at

<https://www.microware.com.br/politicadeseguranca.html>

2.1.2 - CONFIDENTIALITY POLICY

The interested party, Supplier or Customer, and MICROWARE agree unconditionally and irrevocably to consider and treat all information as confidential, consequently, not to disclose to third parties, as well as to protect it in the same way it would protect its own confidential information and not to use it for their own benefit or for the benefit of third parties.

Confidential information encompasses all information written, oral or otherwise presented, whether tangible or intangible, including but not limited to know-how, techniques, designs, specifications, drawings, copies, diagrams, models, flow charts, sketches, reports, forecasts, photographs, computer programs, disks, diskettes, contracts, business plans, processes, projects, specifications, customers, dealer and distributor names, prices and costs, market

9





definitions and information, prices and costs, other technical, financial or commercial information. The references mentioned above are merely illustrative and other instances of confidentiality that exist or may be defined in the future must be kept confidential.

Confidential information will only be disclosed to those employees, directors, representatives, collaborators, and interested parties who have a need to know it for their regular work.

This Commitment binds the heirs and successors of each party to all rights and obligations set forth herein.

2.1.2.1 - PRIVILEGED INFORMATION

Privileged information is understood as any non-public information regarding a public entity.

The use of privileged information is governed by laws, including those that prohibit the improper use of such information.

Microwave has a policy of ensuring compliance with laws to curb improper occurrences.

2.1.2.2 - SECRECY AND CONFIDENTIALITY

Interested parties who have a relationship with Microwave are responsible for preserving confidential or non-confidential information related to Microwave, customers and suppliers as explicitly stated in Microwave's Policies.





2.2 - GOVERNANCE AND ANTI-CORRUPTION

2.2.1 - ANTI-CORRUPTION POLICY

2.2.1.1 - OBJECTIVE AND SCOP

To describe and explain the prohibitions against bribery and corruption and other fraud in all Microwave Tecnologia de Informação Ltda.'s operations (parent company and subsidiaries) establishing guidelines and conduct, ensuring that employees observe the requirements of the Brazilian Anticorruption Law (Federal Law No. 12,846 sanctioned on August 1, 2013) and Decree No. 8420/2015, reinforcing the commitment to conduct its business with the highest standards of honesty and integrity. This Policy should always be interpreted and complied in conjunction with Microwave's Policies.

This Policy applies to all employees, officers, clients, suppliers, partners, and stakeholders who have a relationship with Microwave.

2.2.1.2 - GENERAL CONSIDERATIONS ABOUT THE ANTICORRUPTION LAW

The anti-corruption law, regulated by Decree No. 8420/2015, provides for the administrative and civil liability for acts committed by its employees or third parties acting on its behalf, against the public administration, whether national or foreign.

2.2.1.3 - PROHIBITED CONDUCTS BY THE ANTICORRUPTION LAW

- I. Promising, offering or giving an undue advantage to a public official or a third party connected to them;
- II. Proofably financing, funding or sponsoring the practice of illicit acts;
- III. Hindering investigation or inspection activities by public agencies, entities or agents.





2.2.1.4 - RESPONSIBILITY OF ALL EMPLOYEES

I. The employees must be attentive to situations that may indicate that undue advantages or payments may be occurring, and they must report all suspicious situations to Microwave's Management.

II. The employees must keep special attention to the operations in which the payment or undue benefit may be received by any person, whether a Public Official, including family members, or not, and must report all suspicious situations to Microwave's management.

III. It is the responsibility of all employees to report any violation and/or suspected violation of this Policy.

Reports of violations and suspected violations, whether identified or anonymous, may be made directly to Microwave's management.

2.2.1.5 - RESPONSIBILITY OF ALL INTERESTED PARTIES

I. Suppliers, partners and / or stakeholders who have a relationship with Microwave must know the full content and comply with all the rules of the Anticorruption Law;

II. No supplier, partner and/or stakeholder who does business with Microwave is authorized to offer any benefit on behalf of Microwave, with the purpose of achieving improper benefit, especially in relationship with public officials;

III. No supplier, partner and/or stakeholder who has a business relationship with Microwave is authorized to outsource, assign or share an obligation under an signed contract, without express authorization and previously foreseen in a norm or contract with Microwave (parent company and subsidiaries);

IV. It is the responsibility of all suppliers, partners and/or stakeholders who have a business relationship with Microwave to report any violation and/or suspected violation of the rules of this Policy;





V. Reports of violations and suspected violations, whether identified or anonymous, may be made directly to Microware's Management.

2.2.1.6 - EXAMPLES OF SITUATIONS OF ATTENTION

The following are examples of situations that demand careful analysis:

I. Any refusal to comply with anti-corruption norms;

II. Realization of uncommon procedures or contracting or outside the foreseen procedures, without authorization of exception previously foreseen in Microware's norms (headquarters and branches);

III. Transaction with a third party that has a bad business reputation or refuses to provide all business data;

IV. The employee, supplier or partner and interested party that has a business relationship with Microware that identifies the occurrence of any of these situations, or of any other suspicious situation must, mandatorily, make a report (even if anonymous) to Microware's Management.

2.2.1.7 - CULTURE AND AWARENESS

It is part of the Organizational Culture of Microware (parent company and subsidiaries) not to tolerate the practice of any act of non-compliance with the legislation, especially acts of corruption.

Employees, administrators, suppliers or partners and stakeholders who have a business relationship with Microware (parent company and subsidiaries) have the duty to ensure compliance with anti-corruption norms, as well as this Anti-Corruption Policy, keeping vigilant in relation to the activities and practices of other employees, partner companies, or third parties, reporting suspicious situations to Microware's Management.





All actions, programs, and projects are built and developed based on the best practices and with the strict compliance of the applicable legal system.

2.2.2 - ETHICAL CODE OF CONDUCT

MICROWARE's success over time is based on the principle of ethical conduct of its employees and stakeholders who have a relationship with MICROWARE, who follow the careful observance of laws and Microware Policies, and respect for the highest standards of conduct and ethical integrity.

MICROWARE is based on the idea that all its employees and stakeholders who have a relationship with Microware may sacrifice their integrity, whether to obtain personal advantages or to obtain business benefits.

The Ethical Code of Conduct and Anti-Corruption Policy applies to all employees and stakeholders who have a relationship with Microware.

2.2.2.1- WORK ENVIRONMENT

Microware respects and promotes human rights in its activities. It is committed to having a nondiscriminatory work environment and prohibits discrimination and harassment of any person based on race, color, nationality, creed, religion, age, gender, sexual orientation, disability or any status protected by law.

The diversity of people promotes greater professional and personal experience, contributing to a differentiated service for a range of customers who are also diverse. The application of diversity standards to contracts with suppliers and customers is a demonstration that business is based on quality service, credibility, and price.





2.2.2.2 - BIDDING, PURCHASING AND CONTRACTING

All purchases, contracting, negotiations must be made under the terms of Microware's Policies, Microware's Procurement Policy and/or Management and Contracts Policy (headquarter company and affiliates), being forbidden to contract property and services through the undue use of influence on any person, whether a Public Official or not.

Microware employees and stakeholders who have a relationship with Microware, may not receive or offer any type of gift or entertainment, from any person, individual or legal entity, whether or not a Public Official, that may influence or improperly compensate an act or decision, as an actual or intended compensation for any benefit to the Company and its partners.

2.2.2.2.1 - SPECIFIC SITUATIONS

Participation in Bidding procedures must follow strictly the provisions of the legislation in effect.

All information provided must be true and accurate.

No action aimed at facilitating or circumventing the requirements of the bidding in progress is permitted.

No action, direct or indirect, with any public official or otherwise, is authorized to secure a contract with the intention of securing a contract with Federal, State or Municipal governments, seeking to circumventing competition rules. It is forbidden to do any act with the purpose of:

- I. Frustrate or defraud, upon adjustment, combination or any other expedient, the competitive nature of a public bidding procedure;
- II. Impeding, disturbing or defrauding the performance of any act of a public bidding procedure;
- III. Distracts or tries to distract the bidder, by means of fraud or offering of any type of advantage;
- IV. Fraud public biddings or contracts resulting therefrom;
- V. Create, in a fraudulent or irregular manner, a legal entity to participate in a public bid or administrative contract;
- VI. Obtains an undue advantage or benefit, fraudulently, from modifications or extensions of contracts entered into with the public administration, without authorization by law, in the call for of the public bidding or in the respective contractual instruments;





VII. Manipulating or defrauding the economic-financial balance of the contracts executed with the public administration.

Microware may decide to restrict contracting with the public sector.

Microware (parent company and subsidiaries) and stakeholders who have a relationship with Microware must comply with all laws to which they are bound by the business and activities they practices.

Information requested by tax auditors of any government entity must be responded to truthfully, and you may not offer any advantage to the auditor in order to avoid or impede the inspection, and thus achieve undue benefit.

2.2.2.2.2 – SPONSORSHIP

The sponsorship of events or actions may be done, without offending this policy or the Anticorruption Law, as long as it is not linked to any purpose of undue benefit. In any hypothesis will always be mandatory the approval of Microware's Management, after presentation of a project detailing the values involved, benefits to the business and/or society and information about the sponsored. The project must include background and analysis of profile of the sponsored, with emphasis on the unblemished reputation and non-involvement in situations with suspected or convicted of crimes such as fraud and corruption crimes. Those responsible for the sponsorship proposal will also be responsible for the follow-up of the correct use of the of the assets given as sponsorship. All sponsorships must be based on formalized contracts between Microware (parent company and subsidiaries) and the institutions receiving sponsorship.

2.2.2.2.3 - GIFTS AND HOSPITALITIES

Gifts and hospitalities, understood as gratuities and payment of expenses with entertainment will only be permitted for institutional, commercial or marketing purposes, and always in compliance with the laws, and Microware's Internal Regulations and those of the companies or entities with which Microware maintains relationships.

No gift, gratuity, travel or entertainment may under any circumstances be given to any person, whether or not a Government Official, to improperly influence or compensate an act or decision, as an actual or intended reward for any benefit to Microware (parent company and affiliates), its partners and employees (Own and Third Party).





Any form of gift that is intended to achieve an improper benefit is not permitted.

Are excluded situations in which the institutional or advertising gifts or invitations, thus considered those that display logos and/or products of the company and that are of Nominal value.

Microwave's employees (parent company and affiliates) and stakeholders who have relationships with Microwave are not permitted to accept gratuities, gifts or any benefit of any nature or value from people related in any way to Microwave's corporate activities (contractors, partners, customers, etc.) and in any other way capable of giving the impression that they are intended to obtain or grant an undue benefit.

Employees and stakeholders who have relationships with Microwave that receive benefits or gratuities outside of permitted circumstances must notify Microwave's management, who will evaluate the case of the act and forward the goods, when possible, for donation.

2.2.3 - COMPLIANCE CONTROL OF GOVERNANCE POLICIES

Microwave (parent company and subsidiaries) is committed to promoting ethical and Anticorruption conducts in accordance with current legal order, principles and values assumed in Microwave's Policies.

Employees and stakeholders who have relationships with Microwave should be aware that violations othis Code will be treated with the utmost seriousness and will be susceptible to disciplinary actions, regardless of hierarchical level, without prejudice to legal penalties.

Violations may result in penalties at Microwave's discretion, ranging from a notification to dismissal, always in compliance with applicable civil, labor and criminal laws.

In cases where the violation may cause harms to Microwave, Microwave may seek injunctive lawsuit and claim for damages.

Microwave (parent company and subsidiaries) controls the enforcement of this policy with the use of internal tools, with emphasis on the information coming from the Administration and Audits.

Microwave (parent and affiliates) and stakeholders who have relationships with Microwave must comply with all laws that apply to its business and activities, including international or transnational laws where applicable.





2.2.3.1 - COMMUNICATION CHANNEL

Just as each Collaborator and interested parties who have a relationship with Microware are responsible for their own actions, they may also be responsible for the actions of third parties, if it becomes clear that they knew that these people were violating the Code and did nothing.

Microware (parent company and affiliates) follows best practices in corporate governance, respecting the confidentiality of reports, and protecting whistleblowers by preserving the confidentiality of the information.

Complaints should be sent to:

e-mail: condutaetica@microware.com.br

The confidentiality of anyone who raises concerns and reports will be respected, and retaliation or any embarrassment to its author will not be tolerated.

Website: <https://www.microware.com.br/etica.html>

2.3 - MANAGEMENT OF IT SERVICES

2.3.1 - STANDARD SERVICE LEVEL

This contract is covered by the "Best Effort" Service Level. When Microware operates at this level of service, the service and its completion will be in the best timeline possible within the resources available.

Unless specifically agreed upon between the parties, when the customer plays the role of Supplier, the customer's SLA is best effort and Microware's SLAs are paused while we are waiting on the customer.

For all agreed SLAs, when there is not a specific percentage in the contract Microware's standard percentage of fulfillment is 90%.





With respect to all of Microware's Service Level Agreements (SLAs) with customers, in the event that the customer itself requests/approves a scheduling/service to be performed for a longer time than that foreseen in the agreement, Microware follows the client's request, and adjusts the the client, and adjusts the service level of that specific service proportionally to the time agreed with the client.

2.4 - SUSTAINABILITY POLICY

Microware's Sustainability Policy establishes guidelines that will guide the paths to be followed by all employees and interested parties who have a relationship with Microware on socio-environmental issues and principles for Sustainability in our projects, operations and relations, making explicit our commitment to life and to social, environmental and economic responsibility.

Microware, concerned with the environmental and social impacts of its activities, assumes transparent and responsible ethical conduct in all its relations and negotiations adopting sustainable practices/strategies and conscious actions based on the economic, social and environmental pillars of sustainability.

Microware executes actions and develops projects with the commitment to promote:

- Waste treatment;
- Recycling and selective collection;
- Use of individual, reusable cups and bottles;
- Modernization of IT infrastructure;
- Use of clean and renewable energy;
- Preventive maintenance of hydraulic, electrical and air-conditioning systems;
- Sustainable use of natural resources, especially water;
- Maintaining and supporting activities to raise awareness of the importance of reducing waste, waste management, recycling and saving water and energy.
- Improving the company's internal processes;





- Digital document management;
- Cloud computing;
- Among others.

Microware understands the importance of preserving and maintaining the environment and assumes the commitment to socio-environmental responsible actions that, in addition to contributing to the environment, they also contribute to the company's cost reduction.

3 - TERM OF AGREEMENT

All stakeholders who have a relationship with Microware accept the policies received, or must proactively inform Microware if they do not.

The commitment of all stakeholders is fundamental to this Code of MICROWARE CODE OF ETHICS AND CONDUCT and ESG POLICIES are true instruments of guidance and conduct and be experienced and applied in our daily professional life.

Our integrated Policies can be found at the link: <https://www.microware.com.br/sgi.html>

