MASISA

Corporate Policy

Information Security

INDEX

1. INTRODUCTION

1.1. Purpose

To set out guidelines for the correct use of technology systems, services and platforms, in order to control information security risks, avoid legal and financial problems and guarantee the operational continuity of the business.

Failure to comply with this policy will be considered a serious infraction and disciplinary measures will be adopted in accordance with the internal regulations of the company and the local labor regulations of each country.

1.2. Scope

This policy is part of Masisa's Governance Framework and applies to all its employees (direct and indirect), who make use of services provided by IT.

1.3. Definitions and abbreviations

- **IT**: acronym that identifies information and communications technology services.
- **Information**: interpretation given to certain data, which is part of the company's relevant assets. Said information is confidential and private, so its disclosure to third parties, unauthorized or destruction modification, whether accidental or intentional, must be prevented.
- **Information security**: the level of confidence that the company has in its ability to preserve the confidentiality, integrity and availability of information.
- **IT equipment**: the set of physical devices and software applications that Masisa delivers to its collaborator to carry out their duties.
- **Confidentiality**: meaning that the information is accessed only by authorized persons.
- **Integrity**: an assurance of the accuracy and consistency of the information in its processing, transmission and/or storage.
- **Availability**: providing authorized users with access to information and associated assets, if required.

2. RESPONSIBLE FOR ITS APPLICATION AND FOLLOW-UP

Position	Application	Follow-up
All collaborators	X	
Countries' IT Departments	X	
IT Department		X

3. POLICY DESCRIPTION

- This policy provides the general guidelines that Masisa's collaborators must comply with for the proper use of the technological resources provided by the Company.

.

- The IT Department will monitor the correct use of technological resources and maintain adequate control of information security risks.

- All collaborators must inform the IT Department of their technological requirements, so that together they can evaluate the best technological solution.

- The person responsible for IT in the country must comply with the guidelines of the IT Department and request authorization to incorporate local technologies.

- The country IT manager must enforce this policy and promptly report any breach thereof.

- All purchases of equipment, platforms, applications, software and/or technological services must be evaluated and authorized by the IT Department.

3.1. **Responsibility of the collaborators in information security**

- All collaborators are responsible for maintaining information security, for which they must comply with the recommendations provided by the IT Department.

- Masisa's employees have the duty to protect the company's information.

- All incidents that may affect the security of Masisa's information must be reported immediately to the Local IT or to the IT Department as soon as possible, in order for the respective measures to be taken.

- Any collaborator, who handles technical details of systems, networks, communications, and/or IT infrastructure, cannot reveal said information to third parties, unless they have signed a non-disclosure agreement with, or have been authorized by, Masisa.

- The IT Department is the one who provides the equipment, technological tools and access to the systems for the correct performance of the collaborator's functions.

3.2. **Responsibility of the collaborator in the use of email, internet, licenses and technological equipment**

- The Internet services, email, licenses and technological equipment will be used by the employees, according to the needs of each position, and they will be used only to carry out their business functions or work at Masisa.

- The Internet and/or email cannot be used for purposes that may threaten Masisa's security and/or moral standards and good customs.

3.2.1. **Regarding technological equipment:**

- Any technological tool delivered to a collaborator is the property of Masisa, so it must be used only to carry out his duties.

- The use of the collaborators' own technological equipment is not authorized without the approval of the respective department and of the IT department.

- All collaborators who have assets provided by IT are responsible for their security (passwords and use), and must take care of their user accounts and passwords, not revealing or sharing them with third parties.

- All employment information available in devices provided by Masisa is the property of Masisa.

- The collaborator who has received Masisa's equipment may exceptionally save information of a private nature, taking care that it is separated and duly identified as such.

- Each collaborator is responsible for the care and protection of the equipment that is delivered by the company, and must take all preventive measures to avoid deterioration or major incidents.

3.2.2. **Regarding email:**

- According to the needs of each position, the company will provide an institutional email to carry out the work.

- Collaborators are not authorized to share or transfer information of a confidential or strategic nature to third parties.

- The email must be used only for business purposes, its use for private purposes being prohibited.

- The use of an institutional mail to send information that violates the morals or sensitivity of other people or norms of good customs are prohibited.

3.3. **Regarding the software, platforms, web pages, digital applications:**

- All purchases of software, platforms, applications and/or technological services must be evaluated and authorized by the IT Department.

- Any software that is not licensed, provided and insured through the company's computer services, cannot be used.

- No collaborator is authorized to install, acquire or develop systems, applications, software, websites or any technological component without the formal authorization from IT.

  The IT Department must participate in the cycle of development, implementation and maintenance, with the aim of guaranteeing operational continuity and information security.

4. **VALIDATION**

Function	Name	Position	Date
Prepared by	Rodolfo Lagos	Head of IT Internal Control	November 2019
Reviewed by	Mario Mendez	Head of IT Management	November 2019
Approved by	Georgina Martelli	IT Manager	November 2019
Effective Date: December 2019		Version: 04	

5. **CHANGE CONTROL**

Reason	Responsible	Date
• Update of job titles according to the current structure of the company. • Simplification of the description of the processes. • Updating internal IT processes to adapt them to the new technologies that we are incorporating, maintaining the relevant proper control.	Georgina Martelli Mario Mendez Rodolfo Lagos	December 2019
• Review and general adjustments. • Adds that non-compliance entails disciplinary measures. • The policy is focused on Information Security in the IT field	Georgina Martelli Mario Mendez Rodolfo Lagos	December 2018