MANGO

Information Systems security policy

© MANGO

Updated May 2024

Information Systems security policy

1. Introduction

The use of Information Systems and new technologies have been of great value to MANGO and have contributed, to a large extent, to achieving the levels of business excellence that it currently enjoys. However, as a counterpart to this gain in competitiveness and productivity, they also constitute an important area of risk that can be translated, among others, into external attacks or vulnerabilities, as well as internal abuses or misuses.

The purpose of this document is to set out the basic principles and guidelines relating to the treatment of risks associated with the use of Mango information and/or the systems that host it.

The Board of Directors of Mango orders to have in place security measures and controls that are integrated with Mango's business processes to ensure the confidentiality, integrity and availability of the information in a way that is proportional to the risks and threats.

Mango is understood to be the entire MANGO MNG Holding Group and all the companies that form part of it through a common shareholding relationship.

2. Objective

The main objectives of this policy are listed below:

- Determine and establish the bases for defining the control and management of information, in accordance with the requirements of the business activity, legal, statutory or regulatory requirements, and the obligations assumed in internal contractual contexts and/or with third parties in all areas and wherever Mango operates.
- To have an internal regulatory system for the control and management of information security.
- Establish the principles of risk assessment and risk rating in the area of Information Security.

- To provide Mango's information with adequate and proportional protection based on its confidentiality, integrity and availability regardless of the format, processing system or location in which it is stored.

- To confirm and disseminate among the organisation the relevance that Mango's Management attributes to Information Security.

3. Scope

The contents of this Policy, as well as the regulatory framework that develops it, are mandatory for all employees, collaborators and third parties who access Mango's information, whether they have direct access to the Information Systems or not, since there is a possibility that they may be, even temporarily, in possession of some information support, whether automated and/or on paper or verbally transmitted for some reason. In order to mitigate the risk of transferring confidential data to third parties, confidentiality contracts/clauses exist and will be drawn up, if they do not exist, with all external companies that access company information. These contracts or clauses specify the responsibility of the third party to safeguard the data transferred by Mango and not to assign, disclose or transfer the data without prior notice, as well as to return, destroy or delete the data in the event of termination of the contract.

Particular attention shall be paid to the following cases:

- In those cases in which the Company processes personal data, according to the General Data Protection Regulation, the obligatory nature of compliance with said regulation shall be specified, by reference to Organic Law 3/2018, of 5 December 2018, on Data Protection and Guarantee of Digital Rights.

- PCI-DSS standard compliance (for all employees and third parties who are identified within the PCI environment).

- Compliance with the applicable tax and anti-fraud legislation in the countries where Mango carries out its commercial activity in the development, maintenance and operation of the cash register systems.

- Compliance with the security framework applicable to information systems conducting transactions through the Swift international interbank network.

This Policy, as well as its development and implementation, shall be subject to a review at least once a year to verify its adequacy. This review shall take into account changes in the legal framework in force, the results of audits and risk analyses carried out since the last review.

4. Organisation of information security

The roles and responsibilities for Information Security established to enable the control and protection of Mango Information, as well as to ensure compliance with the objectives and principles defined in this Policy, are as follows:

- **Board of Directors:** endorses, sponsors and gives visibility to the commitment to Information Security, promoting its development, implementation and optimisation, mainly through this Policy and the rules and procedures that develop it.

- **Management Committee:** allocates the necessary resources for the development of the Information Security Plan, approves the necessary budget items for the development of the Information Security Plan, including the necessary awareness and training actions, establishes the level of risk acceptable to Mango, approves the agreements of the Information Security Committee.

- **Information Security Committee**: will guarantee the management of information security in Mango, and will ensure the definition, elaboration, development and control of the activities related to Information Security, analysing the threats, risks and their impact on Mango's operations and processes. It therefore assumes the function of coordinating and establishing the minimum requirements in terms of Information Security and ensuring that all personnel (employees, collaborators and third parties) are aware of the information they handle, its importance and vulnerabilities.

- **Information Systems Management:** responsible for the proper implementation, management and assistance of the computerised systems that support Mango's business processes. To ensure the objectives established in this Policy, it will directly assume the definition, approval, management and control of the implementation of internal procedures and their corresponding monitoring.

- **Users:** Users of Mango Information Systems are responsible for:

(i) Know, understand, accept and comply with the security policy and rules for the use of information systems.

(ii) Process the information solely for the performance of the functions assigned to them, even if their relationship with Mango is not an employment relationship.

(iii) Safeguard the confidentiality, integrity and availability of the information it handles, as well as preserve the secrecy of identifiers and passwords for access to the Information Systems.

(iv) Report to Mango, as soon as possible, any security incident or incident relating to misuse or improper use of information assets of which you become aware.

Staff (employees and third parties) are responsible for protecting information against unauthorised access, modification, disclosure or destruction, whether intentional or accidental.

5. Basic principles

Mango's Information Systems Security Policy is based on the following basic principles that must be complied with:

- Information is an asset of strategic value, so it is necessary to safeguard it from risks that may affect its confidentiality, integrity, availability and traceability, through the application of security measures aligned with business needs and objectives throughout its life cycle, regardless of the system and form of processing.

- Information risks that may materialise should be regularly assessed and reasonable and proportionate measures proposed for their resolution.

- Responsibilities for information security must be adequately defined, based on the established strategy, generating the corresponding organisational structure.
- Protective measures and/or controls should be put in place that are proportionate to the risk and impact to be mitigated.

- The availability of information systems must be ensured, even in emergency situations, both in customer services and internal management, in accordance with the priorities set.

- The information processed and exchanged with natural or legal persons, regardless of its owner, must comply with the requirements in relation to the security of Mango's information, as well as with the applicable legal regulations in force.

- Any person who handles or may handle Mango information must be trained, aware and sensitised to information security and the consequences of non-compliance.

MANGO

© MANGO