

## **INFORMATION SECURITY POLICY**



## 1. Introduction

Mangia's recognizes that information constitutes an essential asset for carrying out its activities, for protecting customers, partners, employees, and all stakeholders, as well as for ensuring the continuity and reliability of its business.

Within its operations – which include organizing and selling tourism services as a tour operator and travel agency, managing infrastructure and services for the tourism sector, and operating hotel facilities – Mangia's processes daily information of a commercial, contractual, operational, organizational, administrative, technological, and personal nature.

This Policy expresses Management's commitment to ensuring that such information is handled in a way that guarantees its confidentiality, integrity, and availability, with the awareness that, for a tourism operator, protecting information also means protecting the trust with which customers, travelers, and guests entrust Mangia's with their travel plans, preferences, and data.

## 2. Purpose

The Information Security Policy defines the general principles, guidelines, and commitments through which Mangia's governs the protection of information and related assets, promoting a structured, aware, and continuously improving approach.

Through its **Information Security Management System (ISMS)**, Mangia's aims to:

- protect information from unauthorized access, alteration, loss, improper disclosure, or unavailability;
- ensure the continuity and reliability of business processes and services;
- prevent negative impacts from IT, organizational, or operational incidents;
- safeguard personal data, commercial information, strategic information, and corporate information assets;

- strengthen the trust of customers, travelers, guests, partners, clients, suppliers, and stakeholders;
- ensure compliance with applicable regulatory, legal, contractual, and organizational requirements.

### **3. Scope**

This Policy applies to all activities, processes, people, systems, tools, and information included within the scope of Mangia's Information Security Management System, relating to:

*“Provision of tourism services as a tour operator and travel agency. Management of infrastructure and services for tourism facilities on behalf of third parties. Management of hotel structures.”*

The Policy applies to all employees, collaborators, partners, suppliers, and, where applicable, to all individuals who access the organization's information or systems.

### **4. Guiding principles**

Mangia's bases its commitment to information security on the following principles:

#### **4.1 Customer focus and protection of trust**

Protecting information is an essential element of service quality. In the tourism sector, every booking, request, preference expressed by the customer, and every piece of information shared in preparation for a trip or stay represents an act of trust that the organization is committed to safeguarding with the utmost care.

Mangia's therefore considers information security an integral part of the customer experience and of its promise of reliability, care, and responsibility.

#### **4.2 Protection of information assets**

All information processed by the organization, regardless of how it is stored or transmitted, must be protected proportionally to its value, sensitivity, criticality, and associated risks.

#### **4.3 Risk-based approach**

Mangia's adopts a systematic approach to risk assessment and treatment, aimed at identifying threats that may compromise information security and implementing appropriate organizational, physical, and technological measures.

#### **4.4 Security throughout the information lifecycle**

Information security is ensured throughout its entire lifecycle: from creation or acquisition to recording, consultation, use, sharing, storage, archiving, and deletion or destruction.

#### **4.5 Need-to-know and authorization**

Access to information must be granted exclusively to authorized individuals, within the limits of actual operational needs and assigned responsibilities.

#### **4.6 Shared responsibility and awareness**

Information security is not solely a technical matter but a shared organizational responsibility. All those working on behalf of Mangia's are required to actively contribute to protecting the information they handle.

#### **4.7 Continuity and resilience**

Mangia's considers it essential to ensure the availability of information and critical services – especially in booking processes, facility management, customer service, and customer relations – even in the presence of adverse events, incidents, or emergencies.

#### **4.8 Compliance and continuous improvement**

The ISMS is maintained, monitored, and continuously improved to ensure alignment with the business context, evolving threats, and applicable regulatory and contractual requirements.

## **5. Organizational Commitments**

To implement this Policy, Mangia's commits to:

- define, implement, maintain, and improve an ISMS compliant with UNI CEI EN ISO/IEC 27001:2022;
- identify and protect business-relevant information, including data relating to customers, travelers, guests, partners, suppliers, clients, and staff;
- classify information and adopt protection measures consistent with its nature and criticality;
- provide enhanced protection for commercial information, personal data, customer profiling data, strategic development information, and confidential organizational, economic, or negotiation-related information;
- ensure adequate controls over physical and logical access, information systems, devices, and document flows;
- promote proper and secure use of digital tools, communication systems, and information platforms;
- prevent, detect, manage, and analyze incidents, anomalies, and events that may compromise information security;
- manage risks arising from suppliers, partners, outsourcing, and third parties handling information or providing relevant services;
- ensure appropriate levels of training, awareness, and staff sensitization;
- adopt measures to support business continuity and resilience of essential services and processes;
- comply with applicable legal, regulatory, and contractual obligations, particularly regarding personal data protection and information security.

## **6. Key Focus Areas for Mangia's**

Mangia's considers the following areas particularly relevant:

- protection of customer, traveler, and guest data and information, as trust is central to the relationship;
- safeguarding commercial information and knowledge related to customer preferences and needs as strategic assets;
- confidentiality of information relating to negotiations, partnerships, business development, acquisitions, and strategic initiatives;
- availability and reliability of information and systems supporting booking, communication, assistance, and facility management;
- security of information flows involving customers, partners, suppliers, clients, and third parties;

- ability to operate resiliently even in contexts characterized by seasonality, high operational volumes, or dependence on digital services and external infrastructures;
- protection of the trust customers place in Mangia's when entrusting their data, preferences, travel needs, and service-related information.

For Mangia's, information security is not limited to technical data protection but contributes concretely to customer relationship quality, service continuity, and the ability to deliver reliable, secure, and market-aligned travel experiences.

## **7. Roles and responsibilities**

Management ensures support for this Policy, promotes a culture of information security, and provides the necessary resources—within organizational and business constraints—for implementing and improving the ISMS.

Relevant business functions, process owners, information owners, and all authorized personnel must:

- apply ISMS rules and related documentation;
- protect entrusted information and tools;
- promptly report events, anomalies, vulnerabilities, or incidents;
- contribute to continuous improvement of the management system.

## **8. Communication, Implementation, and Review**

This Policy is communicated internally, made available to relevant stakeholders, and serves as a reference for defining rules, procedures, and controls within the ISMS.

It is reviewed periodically, and in any case whenever significant changes occur in the context, organization, activities, risks, or applicable requirements, to ensure its ongoing suitability, adequacy, and effectiveness.

## **9. Final Commitment**



Mangia's considers information security not only a compliance requirement but a distinguishing element of its way of operating and a concrete commitment toward customers, travelers, guests, partners, and stakeholders.

In a sector where every experience is built on trust, protecting information also means protecting the peace of mind with which a customer chooses, books, travels, and stays. It means ensuring attention, reliability, and continuity at every stage of the relationship, from the initial request to service delivery.

For Mangia's, information security is part of hospitality, service quality, and the respect owed to every customer. Protecting data means protecting the trust with which each person entrusts the organization with their time, preferences, and travel experience.

PALERMO, 12/05/2025

The Administrator

**Marcello Mangia**  
President & CEO