SECURITY POLICY

Author:	DOSI
Date:	03/06/2024
Version:	v1.0
Classification:	INTERNAL

1. SECURITY POLICY

Proximity, service quality, and guest orientation are our hallmarks. Therefore, aware of the significance of information security, and in line with the path marked by our own identity, **H10** has promoted the establishment of an Information Security Management System in accordance with ISO 27001 requirements. The aim is to identify, evaluate, and minimize the risks to which its information and that of its customers are exposed, as well as to guarantee compliance with established objectives.

The main objective of this Security Policy is to establish an action model that allows us to develop a corporate culture, a way of working, and decision-making at **H10 Hotels**, as well as to ensure that information security and respect for personal data are a constant by:

- Preserving the **confidentiality** of our customer information, preventing its disclosure and access by unauthorized persons.
- Maintaining the **integrity** of our customer information, ensuring its accuracy and preventing its deterioration.
- Ensuring the **availability** of our customer information, on all supports and whenever necessary.

Management, for its part, especially values and establishes the assessment of the availability and confidentiality of its information, and even more so that of its customers, as the main criterion for estimating its risks.

Thus, it is committed to developing, implementing, maintaining, and continually improving its **Information Security Management System (ISMS)** with the goal of continuous improvement in the way we provide our services and in the way we treat our customers' information. Therefore, it is H10's policy that:

- Objectives regarding Information Security are established annually.
- Legal, contractual, and business requirements are met.
- Training and awareness activities regarding Information Security processes are carried out for all personnel.
- A process for risk analysis, management, and treatment of information assets is developed.
- Control objectives and corresponding controls are established to mitigate detected risks.
- Employee responsibility is established regarding the reporting of security violations and compliance with the policies and procedures inherent to the Information Security Management System.

The Security Manager shall be directly responsible for maintaining this policy, providing advice and guidance for its implementation, and correcting deviations in its compliance.

This information security policy shall always be aligned with the company's general policies and those serving as a framework for other internal management systems, such as quality and environmental policies.

Barcelona, June 3, 2024

DOSI Management