BUSINESS CONTINUITY POLICY

Author:	DOSI
Date:	25/11/2025
Version:	v1.1
Classification:	INTERNAL

1. CONTINUITY POLICY

Proximity, service quality, our organization's resilience, and guest orientation are our hallmarks. Therefore, aware of the significance of the continuity of our operations, and in line with the path marked by our own identity, **H10** has promoted the establishment of a Business Continuity Management System in accordance with the requirements of the ISO 22301 standard. The aim is to guarantee the continuity of critical information technology services in the event of disruptions, minimizing the impact on hotel operations and ensuring efficient recovery in compliance with ISO 22301 requirements.

The main objective of this Continuity 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 the continuity of our operations and the resilience of the organization are a constant by:

- Ensuring the availability of critical IT systems in the event of incidents;
- reducing downtime and negative effects on hotel services;
- complying, at all times, with legal, regulatory, and contractual requirements;
- and protecting the company's reputation and the trust of our customers.

Management, for its part, is committed to developing, implementing, maintaining, and continually improving its **Business Continuity Management System (BCMS)** with the goal of continuous improvement in the way we provide our services, as well as to:

- Identify risks and assess their impact on critical services.
- Develop continuity and disaster recovery plans.
- Provide the necessary resources for the implementation of the BCMS.
- Promote a culture of continuous improvement and regulatory compliance.

This policy, as well as the implemented Business Continuity System, is based on the following principles:

- Business Impact Analysis (BIA): Identify critical processes and their technological dependencies.
- Risk Assessment: Determine threats and vulnerabilities that may affect continuity.
- Continuity and Recovery Plans: Document procedures to respond to and recover from incidents.
- Testing and Drills: Regularly validate plans through practical exercises.
- Training and Awareness: Ensure that personnel are prepared to act in the event of a disruption.

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

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

Barcelona, June 12, 2025

DOSI Management