Information Security Policy

1. Introduction

This Information Security Policy (the "Policy") was approved by the Board of Directors of Minor Hotels Europe & Americas in November 2023 and establishes the guidelines for ensuring the confidentiality, integrity and availability of the information processed as part of our business.

For Minor Hotels Europe & Americas and for the people and companies that rely on its services, information is one of the essential assets for achieving its business objectives.

Minor Hotels Europe & Americas team members and management, as well as associates and third parties who provide their services in the course of Minor Hotels Europe & Americas business activities, are subject to the obligations arising from this policy.

Minor Hotels Europe & Americas is committed to complying with the Information Security Policy in accordance with best practices and internationally recognised standards.

2. Objectives

The purpose of this policy is to define the lines of action that make up the corporate strategy of Minor Hotels Europe & Americas in terms of information security, and to develop clear and concise guidelines for the management, protection and proper use of Minor Hotels Europe & Americas information assets.

3. Scope

The scope of the policy includes the information and communication systems, IT services and technologies that support the processes, services and business functions of Minor Hotels Europe & Americas, regardless of the location of the processing operations or the supports or media containing the information.

This policy applies to the following individuals, whether natural or legal persons:

- Employees of all companies that make up Minor Hotels Europe & Americas, regardless of the type of contract governing their employment relationship, the position they hold or their geographical location, including trainees, as well as persons working in hotels under the Minor Hotels Europe & Americas brand (e.g. hotels under management).

- Managers of all Minor Hotels Europe & Americas companies, regardless of the type of contract governing their relationship, position held or geographical location. In any case, the following persons shall be considered as Directors Directors of NH and its subsidiaries,
  - Directors of Minor Hotels Europe & Americas and its subsidiaries,
  - Members of senior management or of the various committees that the Company may have.
- Customers, suppliers or partners, to the extent that this document may be applicable to them and that Minor Hotels Europe & Americas has the capacity to make it effective and enforce it against third parties.

Likewise, the application of all or part of this Policy shall be extended to any other natural and/or legal person that is associated with Minor Hotels Europe & Americas in order to comply with the provisions of this Policy, provided that its application to third parties is possible, depending on the nature of the relationship.

4. Governance

Integrate information security considerations into business decisions as follows:

- The Board of Directors, the highest governing body of Minor Hotels Europe & Americas, is responsible for approving matters related to information security as well as the risk map, including the risk of cyber threats.
- The Management Committee, the body that guarantees the viability of the business, is involved in all decisions related to information security.
- Information Security Executive Committee: to monitor the progress and achievement of the objectives of the Cybersecurity Strategy. Ability to address associated risks and opportunities, as well as provide guidance to senior management on, prioritise and monitor cyber security issues.
- Chief Operations Officer & Global Transformation Leader: Responsible for overseeing the cybersecurity strategy and communicating key cybersecurity issues to senior management. Also chairs the Information Security Executive Committee.
- CISO (Information Security Officer): a senior executive who oversees the cybersecurity of Minor Hotels Europe & Americas and ensures that information technologies and assets are protected against cyber-attacks and/or data leaks. He is also responsible for establishing and monitoring the cybersecurity strategy of Minor Hotels Europe & Americas. He is also a member of the Information Security Committee.
- IT & Systems Department: Coordinate cyber security issues and implement solutions that combine security, sustainability and efficiency. Identify, assess and mitigate potential cyber security risks that could affect the viability of the business.

It also promotes the direct involvement of all members of the organisation, encouraging a proactive, critical and constructive attitude in a constant search for improvement and quality in the processing, development, security and protection of information.

Minor Hotels Europe & Americas is committed to providing the necessary means to achieve the established security objectives, counts on the cooperation of all employees and assumes responsibility for motivating and training them in the knowledge of and compliance with this policy. The management of Minor Hotels Europe & Americas is also committed to supporting the implementation and dissemination of this policy.

5. Commitments

The management of Minor Hotels Europe & Americas is committed to information security management and has established the necessary objectives, responsibilities and behaviours.

The management of Minor Hotels Europe & Americas is responsible for promoting and supporting the establishment of technical, organisational and physical measures to ensure the integrity, availability and confidentiality of Minor Hotels Europe & Americas information in order to prevent possible internal or external threats. The management of Minor Hotels Europe & Americas is responsible for providing the necessary resources to establish the organisational structure, processes, procedures and measures to ensure compliance with applicable laws and regulations and the proper management of information security.

6. Information Security Principles

The policy is developed and implemented through the following guidelines:

- Strategic alignment and vision for the future: all members of the organisation must consider cybersecurity as a fundamental element for the protection of the business and its continuity. Short-, medium- and long-term plans should be established in a cross-cutting manner to achieve the objectives and continuous improvement of cybersecurity.
- Organisation of information security: The application of organisational and technical security measures must be contemplated for all Minor Hotels Europe & Americas information assets, regardless of the physical medium on which they are located and the place from which they are processed. This must be carried out by a duly qualified team, with an adequate allocation of resources, under the direction of the Chief Information Security Officer (CISO). In addition, the organisation's cybersecurity situation should be reported periodically to the governing bodies.
- Human resources security: Mechanisms should be put in place to raise awareness of information security among all Minor Hotels Europe & Americas staff.

- Asset management: Information assets must be classified and responsibilities for them must be assigned.
- Access control: Users must have access only to the resources and information necessary for the performance of their duties. Users are responsible for the confidentiality of Minor Hotels Europe & Americas information and their access credentials.
- Cryptography: Cryptographic keys under the responsibility of Minor Hotels Europe & Americas must be protected.
- Physical and environmental security: Information assets must be located in secure areas, protected by physical access controls and environmental protection systems.
- Operational security: Formalised procedures must be established for the secure management and operation of Minor Hotels Europe & Americas' information systems and technology infrastructure. Regular security assessments should be carried out to anticipate the detection of vulnerabilities before they can be exploited and to encourage continuous improvement.
- Communications security: Communications networks should be designed and implemented to ensure the secure transfer of information, and to comply with the principle of minimum exposure in accordance with risk management.
- Acquisition, development and maintenance of systems: Information security should be considered as part of business as usual, being present from the design phase of any project.
- Supplier relationships: Procedures must be in place to ensure that third parties, who are related to Minor Hotels Europe & Americas and who deal with Minor Hotels Europe & Americas information assets, comply with the policy.
- Information security incident management: Procedures must be defined to detect and respond to incidents that may affect Minor Hotels Europe & Americas' information security, with the aim of being operationally resilient.
- Risk management: Cybersecurity risk management, assessment and communication should be a key element of enterprise risk management across the organisation.
- Information security aspects of business continuity management: Preventive and reactive controls should be in place to ensure the availability of business-critical information resources.
- Compliance and best practice: Ensure that Minor Hotels Europe & Americas' information systems and processing operations comply with applicable laws and regulations and are aligned with best practice guidelines and cybersecurity standards.

7. Structure

The set of normative documents is structured in the following hierarchical model of four (4) typologies of normative documents:

- Policy: the normative document that defines the information security principles to be developed in documents at the following hierarchical levels.

- Standards: Normative documents that define the control objectives and develop each of the information security principles detailed in the Policy.
- Procedures: Normative documents that define the specific actions to be taken to implement the control objectives defined in the standards. These normative documents are derived from the standards or from other procedures.
- Instructions: normative documents that specify how the information security requirements are to be implemented. This category includes manuals, forms and templates. These documents are derived from procedures or other technical work instructions.

All of the above types of regulatory standards are mandatory.
Rules that contradict a higher-level rule are invalid.

8. Monitoring & Information Channel

The policy should be made available to all users of Minor Hotels Europe & Americas information and communication systems. The policy should be posted on the Minor Hotels Europe & Americas employee portal.

Entities that process information owned by or under the responsibility of Minor Hotels Europe & Americas as part of an employment or business relationship must comply with the Policy, acknowledge their responsibility to comply with the Policy and ensure compliance with applicable information security requirements.

All users should express their understanding of their obligations in relation to the Policy.

Incidents and requests for additional information about the Policy can be reported to Information Security by emailing infosec@minor-hotels.com.

9. Compliance

All employees and internal and external partners of Minor Hotels Europe & Americas are responsible for ensuring compliance with the principles of this Policy and Minor Hotels Europe & Americas' internal regulatory documents derived from this Policy, as well as applicable laws and regulations in the field of information security.
User activity on information systems where information owned by or under the responsibility of Minor Hotels Europe & Americas is processed must be monitored and recorded in order to ensure the correct use of information systems and to prevent information security incidents that could jeopardise the security of Minor Hotels Europe & Americas' information assets.
This policy provides a framework for the aspects covered by the following internationally recognised information security standards:

- Information Technology. Security techniques. Information Security Management Systems. Requirements (ISO/IEC 27001).
- Information Technology. Security techniques. Code of Practice for Information Security Controls (ISO/IEC 27002).
- Payment Card Industry Data Security Standard (PCI DSS).

In developing the policy, reference has been made to the legal requirements set out in the laws and regulations of the countries in which Minor Hotels Europe & Americas operates, such as GDPR and national intellectual property (IP) laws. The information security laws and regulations that fall within the scope of this policy are detailed in the Information Security Framework. The recommendations contained in the National Cybersecurity Forum's Cybersecurity Governance Code have also been taken into account.

As Minor Hotels Europe & Americas operates in a number of countries, where the content of this policy differs from national laws and regulations, the most stringent measures and controls will be applied.

Minor Hotels Europe & Americas reserves the right to take legal or disciplinary action in situations of non-compliance with this policy.

In developing the policy, reference has been made to the legal requirements set out in the laws and regulations of the countries in which Minor Hotels Europe & Americas operates, such as GDPR and national intellectual property (IP) laws. The information security laws and regulations that fall within the scope of this policy are detailed in the Information Security Framework. The recommendations contained in the National Cybersecurity Forum's Cybersecurity Governance Code have also been taken into account.

As Minor Hotels Europe & Americas operates in different countries, the most stringent measures and controls will be applied in the event that the content of this policy differs from national laws and regulations.

Minor Hotels Europe & Americas reserves the right to take legal or disciplinary action in situations of non-compliance with this policy.

10. Related Documentation

- Minor Hotels Europe & Americas, S.A. Code of Conduct
- Minor Hotels Europe & Americas, S.A Privacy Policy
- Minor Hotels Europe & Americas, S.A. Sustainability Policy

- Minor Hotels Europe & Americas, Human Rights Policy
- Coperama Code of Conduct
- Minor Hotels Europe & Americas Sustainable Purchasing Commitment

In addition, the Company has two regulatory frameworks for information security that complement this policy and support its proper implementation:

- ALLNH-NOR201-EN - Glossary of Terms and Definitions
- ALLNH-NOR202-EN - Information Security Regulatory Framework

11. Version control

Version	Reviewed by	Approved by	Date
1.0	Department of Information Technology	Steering Committee	December 2013
1.1	Department of Information Technology	Steering Committee	April 2015
1.2	Department of Information Technology	Steering Committee	June 2018
1.3	Department of Information Technology	Steering Committee	November 2018
1.4	Department of Information Technology	Board of Directors	November 2023