Information Security Policy

1. Introduction

This Information Security Policy (hereinafter, the "Policy") was approved by the Management Committee of NH Hotel Group, S.A. (hereinafter, "NH Group" or "NH") in September 2023 and establishes the guidelines to guarantee the confidentiality, integrity and availability of the information processed within the scope of our business.

For NH and for the individuals and companies that depend on its services, information is one of the essential assets for achieving its business objectives.

The team members and management of NH Group, as well as the associates and third parties who provide their services in the development of NH's business activities, are subject to the obligations arising from this policy.

NH Group is committed to complying with the Information Security Policy in accordance with best practices and internationally recognised standards.

2. Objectives

The objective of this policy is to define the lines of action that make up NH's corporate strategy in terms of information security, developing clear and concise guidelines for the management, protection, and proper use of the NH Group's information assets.

3. Scope

The scope of the policy includes the information and communications systems, IT services and technologies that support the processes, services, and business functions of NH Group, regardless of the location of the processing operations or the media or means that contain the information.

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

- **Employees** of all the companies that make up the NH Group, regardless of the type of contract that governs their employment relationship, the position they hold or their geographical location, including interns, as well as people who work in NH-branded hotels (for example, hotels under management).
- Directors of all the companies that make up the NH Group, regardless of the type of contract that governs their relationship, the position they hold or their geographical location. The following persons shall in all cases be considered Directors:
  - Boards of NH and its subsidiaries,
  - Members of the Senior Management or of the various Committees that the Company may have.
- Customers, suppliers or partners, to the extent that this document may apply to them, and NH has the capacity to enforce it and enforce it against third parties.

Likewise, the application of this Policy in whole or in part will be extended to any other natural and/or legal person linked to NH to comply with the provisions of this Policy, provided that it is possible to apply it to third parties, depending on the nature of the relationship.

4. Governance

Integrate information security considerations into business decisions as follows:

- **Management Boards**, NH Hotel Group's highest governing body, is responsible for approving matters related to information security, as well as the Risk Map, including the risk of cyber-threats.
- **Steering Committee**, the body that guarantees the viability of the business, involved in all decisions related to information security.
- **Information Security Executive Committee:** monitoring progress and achievement of the objectives of the cybersecurity strategy. Ability to address related risks and opportunities as well as encourage Senior Management to prioritise and monitor cybersecurity-related issues.
- **Chief Operations Officer & Global Transformation Leader:** responsible for overseeing the Cybersecurity Strategy and communicating material matters related to cybersecurity to Senior Management. Also leads the Information Security Executive Committee.
- **CISO (Information Security Officer):** a high-level executive who oversees NH's cybersecurity and ensures that information technologies and assets are protected against possible cyberattacks and/or data leaks. Is also responsible for establishing and monitoring NH's cybersecurity strategy, and member of the Information Security Committee.
- **IT & Systems Department**: coordinate issues related to cybersecurity, as well as implement solutions that combine security, sustainability, and efficiency. Identify, assess, and mitigate potential cybersecurity-related risks that may affect business viability.

In addition, the direct involvement of all members of the Organization is promoted, fostering a proactive, critical and constructive attitude in the permanent search for improvement and quality in the treatment, evolution, security and safeguarding of information.

NH, committed to providing the necessary means to achieve the established safety objectives, has the collaboration of all employees and assumes responsibility for their motivation and training in their knowledge of and compliance with this Policy. Likewise, NH's Management is committed to supporting its implementation and dissemination.

5. Commitments

NH's management is committed to the management of information security and establishes the necessary objectives, responsibilities and behaviours.

NH's management is responsible for promoting and supporting the establishment of technical, organisational and physical measures that guarantee the integrity, availability and confidentiality of NH's information, in order to avoid possible internal or external threats. NH's Management is responsible for providing the necessary resources for the establishment of the organizational structure, processes, procedures and measures that guarantee compliance with applicable laws and regulations, as well as the correct 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 organization must consider cybersecurity as a fundamental element for the protection of the business and its continuity. Short-, medium- and long-term plans must be established, in a cross-cutting manner, to achieve the objectives and the continuous improvement of cybersecurity.
- Organization of information security: The application of organizational and technical security measures must be contemplated for all NH 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 properly qualified team, and equipped with an appropriate allocation of resources, under the direction of the Chief Information Security Officer (CISO). In addition, the organization's cybersecurity situation must be reported periodically to the governing bodies.
- Human resources security: Mechanisms should be put in place to raise awareness of information security among all NH staff.
- Asset management: Information assets should be classified and responsibilities will be assigned over them.
- Access control: Users must have access only to the resources and information necessary for the performance of their duties. Users must be responsible for the confidentiality of NH information and their login credentials.
- Cryptography: Cryptographic keys under NH's responsibility must be protected.
- Physical and environmental security: Information assets must be located in secure areas, protected by physical access controls and environmental protection systems.
- Operations security: Formalized procedures should be established for the secure management and operation of NH's information systems and technological 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 must 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 part of the usual activity, being present from the design phase of any project.
- Supplier Relations: Procedures should be in place to ensure that third parties, who are related to NH and who deal with NH information assets, comply with the policy.
- Information security incident management: Procedures must be defined to detect and respond to incidents that may affect NH's information security, with the aim of being operationally resilient.
- Risk management: Cybersecurity risk management, assessment, and communication should be a key element in corporate risk management for the entire organization.
- Information security aspects of business continuity management: Preventive and reactive controls must be put in place to ensure the availability of business-critical information resources.
- Compliance and best practices: It must be ensured that the information systems and processing operations carried out by NH comply with current legislation and are aligned with good practice guides 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: This normative document, which sets out the information security principles to be developed in the documents of the following hierarchical levels.
- Standards: Normative documents in which the control objectives are defined, developing each of the information security principles detailed in the policy.
- Procedures: Normative documents that determine the specific actions to be carried out to implement the control objectives defined in the standards. These normative documents emanate from standards or other procedures.
- Work Instructions: Regulatory documents that determine how to apply information security requirements. This category also includes manuals, forms, and templates, among others. These documents emanate from procedures or other technical work instructions.

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

8. Monitoring & Information Channel

The policy must be made known to all users of NH's information and communications systems. The policy must be made known through the NH Employee Portal.

Entities that process information owned or operated by the NH Group, in the context of an employment or business relationship, must adhere to the Policy, acknowledge their responsibility to comply with it, and ensure compliance with applicable information security requirements.

All users must express understanding of their obligations in relation to the policy.

Incidents and requests for additional information about the policy can be reported to Information Security via email infosec@nh-hotels.com.

9. Compliance

All employees, as well as internal and external associates of NH Hotel Group are responsible for ensuring compliance with the principles of the Policy and the internal regulatory documents of NH that emanate from the Policy, as well as with the laws and regulations in force regarding information security.

The activity of users in the information systems, where information owned by NH or under its responsibility is processed, must be monitored and recorded in order to guarantee the correct use of the information systems and prevent information security incidents that may jeopardize the security of NH's information assets.

The policy provides a framework for the aspects covered by the following internationally recognized 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).

For the development of the policy, the legal requirements established in the laws and regulations of the states in which the NH Group operates, such as the GDPR and national laws on intellectual property (IP), have been taken as a reference. The information security legislation and standards within the scope of the policy have been detailed in the Information Security Framework. Likewise, the recommendations contained in the Code of Good Governance of Cybersecurity of the National Cybersecurity Forum have been taken into consideration.

Bearing in mind that NH Group operates in different countries, in the event that the content of the policy differs from national laws and regulations, the measures and controls of the strictest standard will apply.

NH reserves the right to take legal or disciplinary action in situations of non-compliance with the policy.

10. Related Documentation

- NH Hotel Group, S.A. Code of Conduct
- NH Hotel Group, S.A Privacy Policy
- NH Hotel Group, S.A.'s Sustainability Policy
- NH Hotel Group, S.A. Human Rights Policy
- Coperama Code of Conduct
- NH Hotel Group, S.A.'s Sustainable Purchasing Commitment

In addition, the Company has two regulatory frameworks for information security that complement this policy and promote its correct 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	Management Board	November 2023