Information Security Policy

1. Introduction

This Information Security Policy (the "Policy") was approved by the Management Committee of NH Hotel Group, S.A. ("NH Group" or "NH") on July 12, 2023 and establishes the guidelines to assure the confidentiality, integrity and availability of information that undergoes processing in our business.

Information, for NH and for the people and companies that depend on its services, is one of the essential assets for achieving its business goals.

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

NH Group is committed to complying with the Information Security Policy, following best practice and internationally recognized standards.

2. Objectives

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

3. Scope

The scope of application of the policy includes information and communications systems, computer services and the technologies that support the processes, services and business functions of NH Group, independently of the location of the processing operations or of the media containing the information.

This Policy is applicable to the following individuals and companies:

- **Employees** of all the companies that make up NH Group, independently of the type of contract regulating the employment relationship, the post they hold or their geographical location, including interns, and individuals who work in NH brand hotels (for example, hotels under management).
- Executives of all the companies that make up the NH group, independently of the type of contract regulating their relationship, the post they hold or their geographical location. The following will in any case be considered to be Executives:
  - Directors/Board members of NH and its subsidiaries,
  - Members of Senior Management or the various Committees of the Company.

- Customers, suppliers or partners, to the extent that this document may be applicable to them and NH has the capacity to enforce it against third parties.

Furthermore, the application of this Policy, in full or in part, will extend to any other natural and/or legal person linked to NH for the purpose of complying 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

Considerations related to information security are to be integrated in business decisions as follows:

- **Board of Directors,** senior management body of NH Hotel Group, oversees matters related to information security, and approves the Risk map, including the risk of cyber-threats.
- **Management Committee,** the body that assures the viability of the business, is involved in all decisions relating to information security.
- **Information Security Executive Committee:** responsible for monitoring the progress and achievement of the objectives of the cyber security strategy. It has the capacity to address related risks and opportunities as well as to encourage Senior Management on cyber-security related issues and to prioritise and monitor them.
- **Chief Operations Officer & Global Transformation Leader:** responsible for overseeing the Cybersecurity Strategy and for reporting material cybersecurity-related issues to Senior Management. He also chairs the Information Security Executive Committee.
- **CISO (Information Security Officer):** senior executive in charge of cybersecurity at NH and who assures that information technologies and assets are protected from possible cyberattacks and/or data leaks. The CISO is also responsible for establishing and monitoring NH's cybersecurity strategy.
- **IT & Systems Department**: coordinates cybersecurity-related matters, and implements solutions that combine security, sustainability and efficiency. This department identifies, assesses and mitigates possible cybersecurity-related risks that could affect the viability of the business.

The direct involvement of all members of the Organization is also encouraged, fostering a proactive, critical and constructive attitude permanently seeking improvement and quality in the processing, evolution, security and safeguarding of information.

Committed to providing the necessary means to achieve the established security goals, NH has the collaboration of all employees and undertakes responsibility for motivating and training them in knowledge of and compliance with this Policy. NH Management also undertakes to support the implementation and dissemination of the Policy.

5. Commitments

NH Management is committed to information security management and establishes the necessary goals, responsibilities and behavior.

NH Management is responsible for promoting and supporting the establishment of technical, organizational and physical measures that assure the integrity, availability and confidentiality of NH's information, in order to prevent possible internal or external threats. NH Management is responsible for providing the necessary resources to establish the organizational structure, processes, procedures and measures to assure compliance with the applicable laws and regulations, and for proper management of information security.

6. Information Security Principles

The policy is developed and applied through the following principles:

- Information security organization: The application of organizational and technical measures should be considered for all NH's information assets, independently of the physical medium in which they are located and the place from which they are processed.
- Human Resources security: Mechanisms should be established to raise awareness in NH personnel about information security.
- Asset management: Information assets should be classified and responsibilities for them assigned.
- Access control: Users should only have access to the resources and information necessary to perform their duties. Users should be responsible for the confidentiality of NH's information and their access credentials.
- Cryptography: The cryptographic keys under NH's responsibility must be protected.
- Physical and environmental security: Information assets should be located in secure areas, protected by physical access controls and environmental protection systems.
- Security of operations: Formalized procedures should be established for the secure management and operation of NH's information systems and technological infrastructure. Periodic security assessments should be carried out to get ahead of detecting vulnerabilities before they can be exploited and to encourage continuous improvement.
- Security of communications: Communications networks must be designed and implemented to assure the secure transfer of information, and to comply with the risk management principle of minimum exposure.
- Acquisition, development and maintenance of systems: Information security should be considered part of the habitual activity, present from the design phase of any project.
- Relations with suppliers: Procedures should be in place to assure that any third parties that have relations with NH and handle NH information assets comply with the policy.
- Information security incident management: Procedures should be defined to detect and respond to any incident that could affect NH's information security.

- Information security aspects of business continuity management: Preventive and reactive controls should be established to assure the availability of key information resources for the business.
- Compliance: Compliance of NH's information systems and the processing operations carried out by it with ruling legislation should be assured.

7. Structure

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

- Policy: this document, which establishes the information security principles that are to be elaborated on in the documents of the following hierarchical levels.
- Standards: Regulatory documents that define control objectives, developing each of the information security principles detailed in the policy.
- Procedures: Regulatory documents that determine specific actions to be carried out in order to implement the control objectives defined in the standards. These documents emanate from the standards or from other procedures.
- Operating instructions: Regulatory documents that determine how to apply the information security requisites. This category also includes manuals, forms and templates, among others. These documents emanate from procedures or other technical operating instructions.

All the types of regulatory provisions mentioned above are mandatory.
Any provisions that contradict a higher-ranking provision will be invalid.

8. Monitoring and Information Channel

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

Entities that process proprietary information of NH Group or for which NH Group is responsible, in the context of an employment or commercial relationship, must sign up to the Policy, acknowledge their responsibility for complying with it and assure compliance with the applicable information security requisites.

All users must indicate that they understand their obligations in relation to the policy.

Any incidents and requests for additional information on the policy can be communicated to Information Security using the e-mail infosec@nh-hotels.com.

9. Compliance

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

When proprietary information of NH or information for which it is responsible is processed, users' activity in the information system must be monitored and recorded in order to guarantee proper use of the information systems and to prevent information security incidents that could endanger 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. Requisites (ISO/IEC 27001).
- Information technology: Security techniques. Code of good practice for information security controls (ISO/IEC 27002)
- Payment card industry data security standard (PCI DSS).

To develop the policy, the legal requisites established in the laws and regulations of the states in which NH Group does business, such as the GDPR and national laws on intellectual property (IP), have been taken for reference. The information security legislation and standards included in the scope of application of the policy have been detailed in the Information Security Framework.

Bearing in mind that NH Group operates in different countries, in the event that the contents of the policy differ from national laws and regulations, the measures and controls of the stricter regulation shall apply.

NH reserves the right to initiate legal or disciplinary actions in situations of breach of the policy.

10. Related Documents

- NH Hotel Group, S.A. Code of Conduct
- NH Hotel Group, S.A. Privacy Policy
- NH Hotel Group, S.A. Sustainability Policy
- NH Hotel Group, S.A. Human Rights Policy
- Coperama Code of Conduct
- NH Hotel Group, S.A. Sustainable Procurement Policy

In addition, the Company has two information security regulatory frameworks that complement this policy and foster proper implementation of it:

- ALLNH-NOR201-ES – Glossary of terms and definitions
- ALLNH-NOR202-ES – Information Security Regulatory Framework

11. Change History

Version	Reviewed by	Approved by	Date
1.0	Information Technology Department	Management Committee	December 2013
1.1	Information Technology Department	Management Committee	April 2015
1.2	Information Technology Department	Management Committee	June 2018
1.3	Information Technology Department	Management Committee	November 2018
1.4	Information Technology Department	Management Committee	September 2023