nH | HOTEL GROUP

SECURITY POLICY

Document details

Document Name

Security Policy

Document Number

ALLNH-POL100-EN

Version	**Date**	**Status**
1.2	June 2018	Approved
Author	**Content Reviewed by**	**Approved by**
Information Security	Information Security Manager	NH Management
Owner	**Confidentiality Label**	
Information Security	Internal use	

Approval

Charge:	CEO	**Charge:**	Information Security Manager
Name:	Ramón Aragonés	**Name:**	Nuria Lago
Date:		**Date:**	
Signature:		**Signature:**	Nlago

Version Change History

Version	Last Revised	Author	Changes/Comments
1.0	December 2013	Information Technology	Initial version
1.1	April 2015	Information Technology	Corporate Defense AI review
1.2	June 2018	Information Security	Document update

Contents

1. INTRODUCTION

The information is for NH Hotel Group (henceforth, "NH Group" or "NH") and for people and societies that depend on its services, one of the essential assets for achieving their business objectives.

The Information Security Policy (henceforth, the "policy") establishes the guidelines to guarantee the confidentiality, integrity and availability of NH Group's information in accordance with the risk management, proportionality and continuous improvement principles.

As a part of this strategy, NH Management has defined and established through this document the Information Security Policy. NH Management is committed to supporting their deployment and dissemination.

The employees and Management of NH Group, as well as associates and third parties that provide their services carrying out NH business activities, are subject to the obligations arising from this policy.

2. OBJECTIVES

The objective of this policy is to define the action lines that make up NH corporative 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 policy is applicable to the employees of NH Group, its societies and third parties that in the context of an employment or commercial relationship, process information owned by or under the responsibility of NH Group.

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

4. DEFINITIONS

The definitions and terms used in the policy have been detailed in the Glossary of terms and definitions.

5. COMMITMENT OF NH MANAGEMENT

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

NH Management is responsible for promoting and supporting the establishment of technical, organizational and physical measures to guarantee the integrity, availability and confidentiality of NH information, in order to avoid possible internal or external threats. NH Management is responsible for providing the necessary resources for the establishment of the organizational structure, processes, procedures and measures to ensure compliance with the applicable laws and regulations, as well as the proper management of information security.

6. SECURITY POLICY STRUCTURE

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

- Policy: It is the present document. This regulatory document states the information security principles that must be developed in the documents of the following hierarchical levels.
- Standards: Regulatory documents in which the control objectives are defined, developing each of the information security principles detailed in the policy.
- Procedures: Regulatory documents that determine the specific actions to be taken to implement the control objectives defined in the standards. These regulatory documents emanate from standards or other procedures.
- Work instructions: Regulatory documents that determine how to implement 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 above-mentioned typologies of regulatory standards are mandatory.

The rules which contradict a higher-ranking rule shall be invalid.

7. INFORMATION SECURITY PRINCIPLES

The policy is developed and implemented through the following guidelines:

- Organization of information security: The application of organisational and technical security measures must be considered for all NH information assets, regardless of the physical media on which they are located and the location from which they are processed.
- Human resource security: Mechanisms must be put in place to raise awareness of information security issues among NH staff.
- Asset management: Information assets must be classified and responsibilities for them will be assigned.
- Access control: Users must have access only to the necessary resources and information for the performance of their functions. Users must be responsible for the confidentiality of the NH information and their access credentials.
- Cryptography: Cryptographic keys under the responsibility of NH 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 must be established for the secure management and operation of NH's information systems and technology infrastructure. Periodic security assessments must be carried out in order 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 according to risk management.
- System acquisition, development and maintenance: Information security must be considered as part of the 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 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 the security of NH information.
- Information security aspects of business continuity management: Preventive and reactive controls must be established in order to ensure the availability of business-critical information resources.
- Compliance: It must be ensured that the information systems and processing operations performed by NH comply with current legislation.

8. GOVERNANCE

Information Security owns the policy. Information Security is also responsible for ensuring the maintenance, review, development and implementation of the policy throughout NH Group.

Incidents and requests for additional information about the policy may be reported to Information Security via e-mail at infosec@nh-hotels.com

The policy must be reviewed at least annually and updated when significant changes are made to NH's environments.

9. DISSEMINATION

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 by or under the responsibility of NH Group, in the context of an employment or business relationship, must adhere to the policy, recognise their responsibility to comply with the policy, and, ensure compliance with applicable information security requirements.

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

10. COMPLIANCE

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

The user activity in the information systems, where information owned by or under the responsibility of NH is processed, must be monitored and recorded in order to ensure the proper use of information systems and to prevent information security incidents that may endanger the security of NH information assets.

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

The policy provides a framework for 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 where NH Group operates have been taken as a reference, such as the GDPR and national laws about intellectual property (IP). The information security legislation and standards included in the scope of the policy have been detailed in the Information Security Framework.

Considering 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 stricter standard shall be applied.

11. RELATED DOCUMENTS

- ALLNH-NOR201-EN - Glossary of terms and definitions
- ALLNH-NOR202-EN - Information Security Framework