1.0 PURPOSE

The purpose of this policy is to determine the information security rules of Naturel Holding A.Ş. and Group Companies, to ensure that the necessary measures are taken to protect the confidentiality, integrity and accessibility of information with a sustainable understanding and to guide all employees to act in accordance with the policy while performing their duties.

2.0 SCOPE

The Information Security Policy has been determined in accordance with the relevant laws, regulations, Holding policies, Holding values and principles. The Policy, by keeping Information Security at the highest level of importance, covers all Holding stakeholders, including the employees of the Holding and Group Companies, customers, suppliers and business partners, intermediaries, subcontractors, proxy employees and all third party companies with which the Company does business.

3.0 PRINCIPLES

Naturel Holding A.Ş. and Group Companies; in order to meet the information security requirements arising from the national, international or sectoral regulations they are subject to, fulfilling the requirements of the relevant legislation and standards, meeting their obligations arising from agreements, and corporate responsibilities towards internal and external stakeholders; It operates an Information Security Management System compliant with the ISO/IEC 27001 standard for effective management of information security, taking into account the criticality of its information assets.

• Documenting, implementing and continuously improving our information security management system in a way that meets the requirements of the ISO 27001:2022 ISMS standard,
• Protecting the confidentiality, integrity and accessibility elements of information assets,
• Complying with all legal regulations and agreements related to information security,
• Defining current and potential risks in order to ensure information security and systematically evaluating these risks with an effective information security risk management approach,
• Allocating the required competence and adequate resources in terms of ensuring information security, determining institutional roles and responsibilities,
• Providing training to develop technical and behavioral competencies in order to increase information security awareness,
• Defining, operating and taking precautions for processes and scenarios for business continuity, emergency and crisis management,
• Implementing the necessary sanctions in case of information security breach and preventing recurrence;

We work with all our might to be an exemplary organization by managing it in an integrated manner with our other management systems.

4.0 POLICY UPDATES

This policy is reviewed by the Management once a year and updated if deemed necessary.

5.0 REVISION HISTORY

Revision No	Revision Date	Revised Titles	Explanation
00	06.11.2023	-	İlk Yayın
01	06.09.2024	Section 3.0 Principles title is updated.	Revised release