**Durak Hazelnuts**
**Information Security And Risk Evaluation Policy**

As **Durak Hazelnuts**, we recognize the protection of the confidentiality, integrity, and availability of all our information assets, the secure management of our digital and physical information flows, and the uninterrupted continuity of our business operations as fundamental responsibilities. Information security is not only a technical requirement but also an integral part of our corporate reputation, sustainability, legal compliance, and the trust we build with our stakeholders.

Accordingly, the identification, analysis, prioritization, and management of information security risks, together with the implementation of appropriate controls and the transparent governance of these processes, constitute key elements of Durak Hazelnuts' sustainable growth and corporate governance approach. To strengthen information security, manage risks, ensure data confidentiality, and protect all information assets, **Durak Hazelnuts** is committed to:

- Implementing a systematic risk assessment process for all digital and physical information assets.
- Classifying information assets according to their level of importance and reviewing them regularly.
- Identifying and assessing threats, including unauthorized access, data loss, data leakage, cyberattacks, hardware failures, and human error.
- Prioritizing and managing information security risks based on their likelihood and potential impact.
- Implementing effective technical and organizational controls, including strong password policies, antivirus protection, firewalls, access authorization, multi-factor authentication, backup systems, and log monitoring.
- Restricting access to critical information in accordance with the **need-to-know principle**.
- Raising employees' awareness of information security through regular training and ensuring full compliance with this policy.
- Continuously enhancing the security of the company's email systems, cloud services, mobile devices, and network infrastructure.
- Requiring third-party service providers and business partners to comply with our information security standards and implementing corrective actions in cases of non-compliance.
- Complying with the Turkish Personal Data Protection Law (KVKK) and all other applicable national and international information security regulations.
- Reviewing and updating information security risk assessments at least annually and conducting additional risk assessments whenever new systems, software, projects, or platforms are introduced.
- Ensuring that any information security incident, suspected breach, or identified vulnerability is investigated promptly, securely, and with due regard for confidentiality.
- Ensuring that this Information Security Policy is implemented in an integrated manner with our Code of Ethics, Privacy Policy, Conflict of Interest Policy, and other relevant procedures.
- Continuously improving this policy in line with changes in legislation, industry risks, technological developments, and the evolving needs of the company.

We are committed to implementing and continually improving our Information Security And Risk Assessment Policy to achieve these principles.