Doğan Şirketler Grubu Holding A.Ş.
Information Security Policy

Doğan Şirketler Grubu Holding A.Ş. (the "Company") *Information Security Policy* ("Policy") sets out the general principles and procedures for ensuring the confidentiality, integrity, and availability of information in connection with the establishment, operation, management, and use of information systems.

The objectives of this *Information Security Policy* are to define the roles and responsibilities required for the effective operation of information security processes; to assign relevant responsibilities; to design processes for managing risks related to information systems; to implement appropriate controls; to conduct the necessary assessments; and to ensure ongoing monitoring.

A) Key Roles, Responsibilities, and Job Descriptions related to Information Systems

1. Board of Directors

The Company's Board of Directors reviews the *Information Security Policy* prepared by Senior Management in line with the general principles, procedures, and objectives relating to information systems and grants final approval.

Under this *Policy*, the Board of Directors is responsible for establishing, evaluating, and overseeing effective, adequate, and compliant information systems controls.

2. Senior Management

The Company's Senior Management oversees the implementation of the *Information Security Policy* and the information systems strategy.

The responsibilities of Senior Management include setting information security objectives; assigning duties in accordance with the principle of *segregation of duties*; allocating the necessary resources for the effective and coordinated management of information systems; and granting final approval for policies, procedures, processes, or projects within their scope of authority.

3. Information Systems Unit

The Company's Information Systems Unit is responsible for managing the implementation of the *Information Security Policy* and the information systems strategy.

The Information Systems Unit is tasked with:

- Establishing and continuously improving processes and controls related to information systems management.
- Assessing security risks arising from information systems.
- Implementing appropriate mechanisms to maintain information security controls at an adequate and effective level.

- Ensuring that information security processes are aligned with the ISO/IEC 27001 standard.

4. Employees and Other Stakeholders

All Company employees, as well as other stakeholders - including suppliers, customers, business partners, service providers, and consultants who access or use the Company's information and business systems - are required to comply with this *Information Security Policy* and the information systems strategy. They are expected to participate in training activities aimed at increasing awareness of information security requirements, risks, and current threats, and to report any suspected or actual information security incidents.

B) Objectives for Information Systems

Information systems are considered a key component of the Company's corporate governance practices and management structure. **In principle**, the objectives include:

- Ensuring that information systems strategies are aligned with business objectives, enabling Company operations to be conducted in a stable, competitive, continuously developing, and secure manner.
- Managing information systems effectively by ensuring their security, performance, efficiency, accuracy, and continuity.
- Ensuring the confidentiality, integrity, and availability of information, as required.
- Maximizing compliance with applicable legislation, standards, and contractual obligations.
- Minimizing information security threats and incidents through the implementation of effective and up-to-date information security controls.
- Enhancing the level of awareness, understanding, and compliance of employees and stakeholders with respect to information systems and information security.

C) Processes and Controls for Managing Information Systems Risks

This *Information Security Policy* governs the general principles and procedures related to the management of information systems, while the detailed processes and controls for managing information systems risks are defined in the relevant internal procedures.

The *Information Security Policy* and related procedures are reviewed periodically and updated as necessary to ensure compliance with legal and regulatory requirements, address newly emerging risks and threats, and reflect changes in the Company's business models and organizational structure within existing processes and controls.