DOĞANLAR
HOLDİNG

INFORMATION SECURITY POLICY

Information classification guidelines have been established at Doğanlar Yatırım Holding A.Ş. in order to raise corporate awareness on information that has sensitivity at various levels in terms of confidentiality as part of information security activities, to determine and implement logical, physical and administrative controls suggested for information that has various sensitivity levels, and to identify the storage and destruction rules for data kept in portable environments.

We undertake the following for the implementation, revision and constant improvement of applications related to Information Security;

- To identify risk acceptance criteria and risks, and to improve and implement controls,
- To ensure the implementation of information security risk assessment process with a view to determining the risks related to harm to confidentiality, integrity and accessibility of information within the scope of information security management system, and to identify risk owners,
- To define the framework for assessment of confidentiality, integrity and accessibility impact of the information covered by the scope of information security management system,
- As a company, we are committed to handling personal data in compliance with national and international regulations, including the KVKK (Personal Data Protection Law), to ensure the protection and confidentiality of personal data. We are meticulous in processing, storing, and disposing of personal data in accordance with these regulations.
- We aim to detail our information security management system to encompass all necessary technical and administrative measures to safeguard the integrity, confidentiality, and accessibility of personal data. Within this framework, we develop transparent processes to protect the rights of data subjects and regularly review and enhance these processes.
- To revise the technological expectations within the scope of the service provided, and constantly follow-up risks,
- To meet information security requirements arising from applicable national or sectoral regulations, the requirement to fulfill the obligations under legal and applicable legislation and contracts, and the corporate responsibility towards internal and external stakeholders,
- To minimize the impact of information security threats to service continuity, and contribute to business continuity,
- To have the required competence for fast response to potential information security incidents and minimizing the impact of the incident,
- To maintain and improve information security level over time with a cost-efficient control infrastructure,
- To improve corporate reputation and ensure protection against negative impact related to information security.
- As a company, we aim to integrate awareness of environmental sustainability and climate change mitigation into our technological processes and information security practices.
- Within the scope of our information security management system, we prioritize solutions that reduce energy consumption, minimize our carbon footprint, and preserve natural resources. In this context, we aim to mitigate environmental impact, combat climate change, and thus ensure both information security and fulfill our environmental responsibilities.