INFORMATION SECURITY POLICY

- Specifying risk acceptance criteria and risks, developing and applying controls.
- Enforcing information security risk assessment process to specify risks regarding confidentiality, integrity and accessibility losses within the scope of information security management system, specifying risk holders.
- Defining a framework to assess confidentiality, integrity and accessibility impact within the scope of information security management system.
- Revising technological expectations within the context of related services, and conducting close follow-up of risks.
- Covering information security requirements arising from the binding national or sectoral arrangements, compliance with legal or related regulations, the coverage of obligations resulting from agreements, corporate responsibilities towards internal and external stakeholders.
- Mitigating information security threats towards the realization of continuous services, and contributing to service sustainability.
- Having the competence to rapidly intervene in possible information security incidents, and minimize the impact of particular incidents.
- Maintaining and ameliorating the level of information security with a cost-efficient control infrastructure.
- Improving corporate credibility, permanently protecting information security from adverse impacts.

An information classification guideline is designed to raise corporate awareness regarding information with different levels of sensitivity in terms of confidentiality within the scope of **Doğanlar Holding** information security system, to specify and apply logical, physical and administrative controls suggested to be implemented for these different sensitivity levels, and to define storage and purge criteria for data in transferable environments.

Doğanlar Holding Higher Management commits to execute, revise and constantly improve Information Security, and conduct all related implementations.