INFORMATION SECURITY POLICY

As the Performance Group;

• To determine risk acceptance criteria and risks, to develop and implement controls,

• To ensure the implementation of the information security risk assessment process to identify risks related to confidentiality, integrity and accessibility losses of information within the scope of the information security management system, to determine risk owners,

• To define a framework for evaluating the confidentiality, integrity and accessibility effects of information within the scope of the information security management system,

• To continuously monitor risks by reviewing technological expectations within the context of the scope of the service provided,

• To meet information security requirements arising from national or sectoral regulations, legal and relevant legislative requirements to which we are subject, to meet obligations arising from agreements, and corporate responsibilities towards internal and external stakeholders,

• To reduce the impact of information security threats on service continuity and contribute to continuity,

• To have the competence to rapidly intervene in information security incidents that may occur and to minimize the impact of the incident,

• To maintain and improve the level of information security over time with a cost-effective control infrastructure.

• To develop the reputation of the institution and to protect it from negative impacts based on information security,

we are commited.