Security Policy of information

- To manage information assets, to determine security values, needs and risks of assets, to develop and implement controls on security risks.
- Define the framework for determining the information assets, values, security needs, vulnerabilities, frequency of threats to assets.
- Define a framework for assessing the effects of threats on the confidentiality, integrity, and accessibility of assets.
- To demonstrate working principles for the handling of risks.
- To continuously watch the risks by reviewing technological expectations in the comprehensive complex served
- Providing information security requirements arising from the national or sectoral regulations it is subject to, fulfilling the requirements of legal and relevant legislation, meeting the obligations arising from the agreements, and corporate responsibilities towards internal and external stakeholders.
- Reducing the impact of information security threats to service continuity and contributing to continuity.
- To have the competency to intervene rapidly and to minimize the impact of the event.
- To maintain and improve a cost effective control infrastructure and information security level in time.
- To improve the reputation of the institution, to protect against the negative effects of information security.

General Manager