

Information Security Management System Policy

To determine the security principles for the corporate information and portfolios, Tüpraş commits

- to protect integrity, accessibility and confidentiality of data
- to protect reliability and corporate reputation
- to ensure security of portfolios effectively
- to ensure conformity with the national and international regulations related to the information security
- to implement the emergency action plan in cases of emergency ensuring continuation of the primary and supportive business operations with the minimum interruption
- to make much more effective continuous improvement by managing risks of information security as to our business processes
- to put the users under obligation in relation to the information security by creating awareness on the employees, suppliers and associates
- to provide support of the management for implementation, continuous improvement, control of the Information Security Management System and imposing necessary sanctions in case of security violations.



İbrahim Yelmenoğlu
General Manager

Supplier Information Security Code of Conduct;

The Supplier;

- ✓ Take the utmost care to protect the information obtained or to be obtained from its products, activities and services and must protect this information with appropriate security measures.
- ✓ Intellectual property rights must be respected.
- ✓ Technology and acquired knowledge transfer should be done in a way that protects intellectual property rights.
- ✓ Protect the information of its employees, customers and suppliers.
- ✓ It should record information security incidents that occur within the scope of the service provided and provide support in the elimination of these incidents.
- ✓ Evaluate information security risks related to information and communication technology services and product supply chain and raise awareness for its employees.
- ✓ Responsible for keeping contact information up to date.