As Enerjisa Üretim and Control, Monitoring and Development Room (Senkron), we adopt the following principles regarding information security management in order to become an energy company that continuously improves its know-how, sets standards and shapes the future of the sector.

- We ensure that our information resources and processes comply with the principles of confidentiality, integrity and accessibility.

- We ensure the security of all industrial control systems, corporate information systems and information assets used for the generation of electrical energy against unauthorized access and change.

- We ensure the security of all kinds of personal data, commercial and financial information belonging to our company, stakeholders and employees and take preventive measures to prevent leakage.

- We comply with all applicable laws, regulations, contractual obligations, industry standards and other relevant internal and external requirements related to information security and make continuous improvements.

We ensure standardization by the Central Operation, Control, Monitoring and Development Room (Senkron) for power plant operation and performance monitoring with remote access. Enerjisa Üretim and Senkron management provides the necessary resources, assigns and directs the necessary resources for the implementation and sustainability of the information security management system (ISMS).

At Enerjisa Üretim and Senkron, all the employees are responsible for compliance with policies, procedures and instructions to ensure Information Security.

As all Enerjisa Üretim and Senkron employees, we undertake to realize information security for the following purposes by protecting the confidentiality, integrity and accessibility of our company's information assets and processes.

- We determine all roles and responsibilities related to information security with the support of management and coordination of units.

- We set and measure information security targets and evaluate opportunities for improvement.

- We analyze information security risks and opportunities, plan and implement remedial actions related to these risks and opportunities.

- We carry out continuous awareness-raising and training activities to increase the awareness of all employees and relevant stakeholders on Information Security.

- We develop business continuity plans to ensure the continuity of critical systems and processes.

- We ensure that information security incidents are reported by all employees and relevant parties and we take the necessary measures to prevent recurrence.