



INFORMATION SECURITY AND CRITICAL INFRASTRUCTURE CYBERSECURITY POLICY

As one of the leading power generation companies in Turkish Energy Sector, to manage the risks arising from all kinds of cyber attacks against our business continuity, information assets and industrial control systems;

We are committed;

COMPLIANCE WITH STANDARDS

To establish and implement an Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - which provides confidentiality, integrity and availability of our assets according to ISO / IEC 27001:2022 standard, Security techniques Information security controls for the energy utility industry according to ISO/IEC 27019:2020

LEGAL COMPLIANCE

To comply with all legal requirements regarding information security and other contractual terms specific to the energy sector, which includes critical infrastructures,

RISK AND OPPORTUNITY ASSESSMENT

Managing the risks that may occur on our information assets, industrial control systems and all connected critical infrastructures by evaluating them according to confidentiality, integrity and accessibility, and to identify opportunities,

AWARENESS

Performing trainings, in order to increase the awareness of information security and cybersecurity,

SUBCONTRACTORS AND SUPPLIERS

Provide appropriate awareness training about corporate policies and procedures related to their own job functions, agreeing information security requirements with our suppliers to reduce risks related to unauthorized access of our suppliers to the organization's assets.

CONTINUOUS IMPROVEMENT

In line with our company goals, we aim to manage information security risks and opportunities in an integrated manner with other management systems by creating a constantly improving and developing structure that does not allow the emergence of new risks.

Özge ÖZEN AKSOY
Chief / Financial Officer



Can GÜLCAN
Deputy General Manager



Serhan GENÇER
General Manager

