

INFORMATION SECURITY AND CRITICAL INFRASTRUCTURES CYBER SECURITY POLICY

As one of the leading electricity generation companies in Türkiye's energy sector, and in order to manage risks arising from all types of cyber attacks against our business continuity, information assets, processes, and industrial control systems, we commit to the following:

To establish a framework for the determination, implementation, and review of information security objectives, to protect the continuity of energy supply, and to ensure the security of our critical infrastructure,

COMPLIANCE WITH STANDARDS

To establish, implement, maintain, and continually improve an Information Security Management System that safeguards the confidentiality, integrity, and availability of our assets in compliance with the requirements of TS ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management System and TS ISO/IEC 27019:2020 Information Technology - Security Techniques - Information Security Controls for the Energy Utility Industry standards,

To ensure that the operational technology (OT) and supporting information technology infrastructures in our energy production facilities are managed in accordance with information security principles,

COMPLIANCE WITH LEGAL AND OTHER REQUIREMENTS

To protect all our information assets and digital infrastructure in line with applicable best practices and recognized frameworks,

To comply with all applicable legal requirements related to information security and other contractual requirements specific to the energy sector hosting critical infrastructure, and to fulfill other applicable obligations,

RISK AND OPPORTUNITY ASSESSMENT

To assess and manage risks that may arise in relation to our information assets, industrial control systems, and all related critical infrastructure in terms of confidentiality, integrity, and availability, and to identify opportunities,

AWARENESS

To conduct training activities to increase information security and cybersecurity awareness,

To implement regular awareness and drill programs to enhance the information security awareness of all our employees, contractors, and suppliers,

CONTRACTORS AND SUPPLIERS

To provide appropriate awareness training on corporate policies and procedures relevant to their respective business functions,

To define and agree on information security requirements with our suppliers in order to reduce risks related to unauthorized access to the organization's assets, and to ensure that these requirements are monitored through contractual obligations and audit mechanisms,

CONTINUAL IMPROVEMENT

We commit to managing information security risks and opportunities in integration with other management systems in line with our corporate objectives, to continually improving the effectiveness of our Information Security Management System, and to keeping our processes up to date by following technological developments specific to the energy sector.



Harun TAŞ

Power Generation Assistant General Manager



Hakan YILDIRIM

General Manager

