
GLOBAL INFORMATION SECURITY POLICY



TABLE OF CONTENTS

INTRODUCTION	2
1. PURPOSE	2
2. SCOPE	2
3. MAIN PRINCIPLES	2

INTRODUCTION

We know the importance of a consistent, effective and transparent communication model to achieve global success in line with our organizational goals. For this reason, we have established a comprehensive Global Information Security Policy to communicate with all our stakeholders in an open, transparent and reliable manner. In this way, we follow the technological developments that are in rapid motion today and guide our processes with a measurable, transparently reportable and auditable information security system that complies with international standards.

1. PURPOSE

The objective of this policy is to ensure the protection of all information assets in accordance with the principles of confidentiality, integrity, and availability; to effectively manage physical and cybersecurity risks that may arise in critical systems, including IT and OT/SCADA environments; and to define the minimum information security principles to be complied with.

2. SCOPE

This policy applies to all employees, contractor personnel, temporary workers, interns, consultants, visitors, and all third parties with access to information systems working at Aksa Energy and our subsidiaries.

3. MAIN PRINCIPLES

- Our Company establishes, operates, periodically reviews, and continually improves a risk- and process-oriented global Information Security Management System compliant with national and international regulations and standards, aligned with ISO/IEC 27001:2022 and energy sector-specific ISO/IEC 27019 standards, which is measurable, reportable, and auditable.
- Our Company complies with all legal regulations and contractual requirements in the field of information security, regularly monitors these requirements, and continuously enhances its compliance processes.
- By keeping pace with continuous changes and developments in technology, our Company develops its organizational, process, technology, and audit capabilities, and applies the PDCA (Plan-Do-Check-Act) approach.

- Our Company bases all decision-making and business processes on information security principles, determines information security objectives in alignment with business objectives, and addresses them as an integral part of our corporate strategy.
- Our Company determines the duties, roles, and responsibilities as well as the necessary resources within the scope of information security.
- Our Company ensures that all kinds of corporate and personal data are;
 - confidential and accessed only by authorised personnel,
 - accurate and complete and in integrity in order to keep changes under control,
 - accessible and protected so that authorised persons can use it whenever they need it.
- Our Company identifies information assets, assess the risks related to confidentiality, integrity, accessibility and other principles of these assets, implement risk management activities and establish the necessary control points for mitigation
- Our Company ensures access management in line with the principle of least privilege and the Zero Trust approach; continuously performs identity, authorization, and device verification.
- Our Company implements technical and administrative measures, such as logging, access control, data retention, masking, encryption, and disposal, to protect information assets.
- Our Company protects all critical information assets, particularly customer information, in a secure, traceable, and manageable manner; takes into account the information security expectations of internal and external stakeholders.
- Our Company defines processes and scenarios for business continuity, emergency, and crisis management; develops, implements, and regularly tests these plans to ensure the uninterrupted operation of critical processes and systems.
- Our Company establishes the necessary systems to effectively manage information security breaches and vulnerabilities; implements corrective and preventive actions to minimize the impact of breaches and prevent their recurrence. Our Company conducts incident response processes in an integrated manner with business continuity and emergency management.
- Our Company identifies, analyzes, prioritizes, and manages threats and vulnerabilities related to industrial control systems and corporate information systems in accordance with applicable legislation and standards to ensure their security and continuity.
- Our Company takes proactive action in cybersecurity processes by using reliable national and international threat intelligence sources.

- Our Company ensures that this Policy is communicated, accessible, understood, and effectively implemented.
- Our Company plans and conducts regular training for our employees, business partners, and other stakeholders to increase information security awareness and make it an integral part of the corporate culture.
- Our Company expects and monitors all business partners to comply with the information security legislation of the countries in which we operate and to act in accordance with this Policy.

Release Date: 07.10.2026

Revision Date: -

Rev:00

Our Corporate Governance Policies are one of the cornerstones of our strategy and an integral part of our business culture.

