**Purpose**

The purpose of this policy is to ensure the security of all information assets within Arslan Alüminyum A.Ş.—including human resources, infrastructure, software, hardware, customer information, corporate records, third-party data, and financial assets; to effectively manage information security risks; to monitor the performance of information security management processes; and to regulate information security regarding third-party relationships.

**Scope**

This policy encompasses all departments, employees, subcontractors, suppliers, business partners, and all relevant parties with access to information at Arslan Alüminyum A.Ş. In addition to data stored in electronic environments, it includes written, printed, verbal, and all other forms of information media.

**Responsibilities**

The **ISMS Team** is responsible for the establishment, implementation, maintenance, and continual improvement of the Information Security Management System (ISMS). All employees are obligated to comply with the requirements of this policy, participate in information security awareness training, and report potential security breaches or incidents to the ISMS Team. **Top Management** is responsible for providing the resources required to support information security and ensuring that necessary preventive measures are taken.

**Principles and Commitments**

- As Arslan Alüminyum A.Ş., we commit to the following principles:
- **Asset Protection:** We protect our information assets against all threats, whether internal or external, intentional or accidental.
- **Integration and Compliance:** We manage information accessibility in an integrated manner with business processes, ensuring full compliance with legal, regulatory, and statutory requirements.
- **The CIA Triad:** We base our framework on the continuity of the three core pillars of the Information Security Management System:
- **Confidentiality:** Preventing unauthorized access to information.
- **Integrity:** Preserving the accuracy and completeness of information.
- **Availability:** Ensuring authorized users have seamless access to information when required by business needs.
- **Comprehensive Mediums:** Information security is not limited solely to electronic data but encompasses all physical and digital environments.
- **Awareness Cultivation:** We strengthen corporate consciousness by providing regular information security awareness training to all personnel.
- **Vulnerability Handling:** We encourage the reporting of actual or potential information security vulnerabilities to the ISMS Team, executing necessary investigations and corrective actions.
- **Business Continuity:** We establish, test, and maintain business continuity plans to ensure an infrastructure resilient against emergencies and disruptions.

- **Risk Management:** We periodically evaluate information security risks, formulate comprehensive action plans, and systematically track their execution.
- **Contractual Safeguards:** We take regulatory and preventative measures to prevent disputes or conflicts of interest that may arise from agreements between parties.
- **Access Control Management:** We ensure that information systems and user access rights are managed strictly in accordance with business requirements and the "least privilege" principle.
- **Secure Third-Party Management:** We base our relationships on secure management principles regarding cloud computing, outsourcing, and third-party service providers.
- **Cybersecurity Defenses:** We implement rigorous technical and organizational measures against evolving siber security threats.
- **Sustainability & Environmental Assessment:** We evaluate the potential impacts of environmental factors—such as global climate change, resource scarcity, and sustainability—on information security infrastructure.
- **Stakeholder Expectations:** We monitor the changing needs and expectations of interested parties and update our policy framework accordingly.
- **ISO 27001 Alignment:** We adopt a continual improvement approach in strict compliance with the **ISO 27001:2022** standards.
- **Holistic Strategy:** We view information security not merely as a technological matter, but as an integral part of corporate sustainability, reputable business conduct, and social responsibility.

**Implementation**
The Information Security Management System is executed across all activities of Arslan Alüminyum and operates in an integrated manner with other management systems. The ISMS Team secures the effectiveness of the system through systematic risk analyses, awareness training, internal audits, and technical controls.

**Monitoring and Review**
ISMS performance is systematically monitored through periodic risk assessments, internal audits, management reviews, and security incident analyses. Based on the data points and outputs obtained, the policy is periodically reviewed, updated, and continual improvement activities are executed.

**Effective and Review Dates**
**Effective Date:** 12.02.2026
**Review Date:** 12.02.2027