

1. Purpose and Scope of Information Security and Management Commitment

Ahlatcı Metal Rafineri considers corporate information to be an extremely valuable asset. Information is critical for the sustainability of our business activities and must be protected appropriately. By implementing the **ISO 27001** standard, the Ahlatcı Metal Rafineri Information Security Management System (ISMS) aims to minimize the risks—and the potential impacts of those risks—related to the **Confidentiality, Integrity, and Availability** of corporate information.

This policy has been approved by the senior management of Ahlatcı Metal Rafineri. The senior management has committed to the fulfillment of the following objectives:

- Ensuring the confidentiality, integrity, and availability of Ahlatcı Metal Rafineri's information and information systems.
- Identifying risks to information assets and managing these risks systematically.
- Fulfilling the requirements of Information Security Standards.
- Complying with all legal regulations related to Information Security.
- Evaluating and implementing continuous improvement opportunities to sustain the Information Security Management System.
- Conducting training sessions to enhance technical and behavioral competencies and increase information security awareness.
- Ensuring that sub-procedures related to this policy are prepared and published by the Information and Communication Technologies (ICT) officers.

The Ahlatcı Metal Rafineri Information Security Policies are valid and mandatory for all personnel—whether full-time, part-time, permanent, or contracted—who use corporate information or business systems, regardless of geographical location or business unit. All third-party service providers and their affiliated support personnel who require access to corporate information must also adhere to the general principles of this policy and other security responsibilities and obligations they are bound by.

2. Responsibilities of All Employees

The purpose of Information Security and this policy is to protect, maintain, and manage the confidentiality, integrity, and availability of information and all supporting business systems, processes, and applications. This means ensuring that Ahlatcı Metal Rafineri's information remains in authorized hands; that information is complete, accurate, and usable; and that information and systems are ready for use when

needed. Therefore, all corporate and outsourced personnel, as well as interns—regardless of their position or duties—are responsible for performing their work in a manner that ensures the protection of information within the organization.

In addition to ensuring that Ahlatcı Metal Rafineri's information is complete, accurate, and available, all personnel must comply with the protection of confidential information as specified in the Personnel Rules and the corporate Principles of Business Ethics.

Ahlatcı Metal Rafineri undertakes to take the measures specified in the **Law on the Protection of Personal Data (KVKK)** and to operate in full compliance with the Personal Data Protection Policy. The confidentiality of personal and corporate information is ensured and is not shared with other corporate entities or individuals. Access to data is restricted, and all access is logged.

3. Policy Ownership and Guidance on Information Security

The functional ownership of this policy, all standards, other supporting documents, and training activities will be carried out by the **Information Security Management**. This management will also serve as a source of advice and a guide regarding the implementation of the policy throughout the organization.

Information Security Management will ensure that all employees receive appropriate training to achieve a suitable level of awareness regarding Information Security issues and will provide guidance on handling information security incidents in general. When necessary, it will ensure that this policy is supported by detailed standards, procedures, and processes, and that these are available for use as needed. Furthermore, it will be responsible for communicating the requirements of this policy to all employees (permanent or temporary) and all contractor personnel.

The **Information and Communication Technologies Manager** will be responsible for establishing and maintaining the general management framework for Information Security. They will also ensure that this policy is continuously reviewed to remain up-to-date and reflect the business requirements of corporate affiliates or changes in the risk environment and threats facing information and information systems.

Information Security policies are reviewed at least once a year, in parallel with asset and risk updates conducted to reflect the current risks facing Ahlatcı Metal Rafineri's information assets. To keep new risks and changes in existing risks under control, Information Security Policies are updated with necessary additions. Additionally, any

employee may request a policy change from the Information Security Management to improve the policies and better reflect the controls needed by the institution. Such requests are handled and evaluated by the Information Security Management.

Information Security Policy principles must be applied in parallel with the Personnel Rules of Ahlatcı Metal Rafineri Human Resources. Employees are also responsible for being aware of the Information Security Policy and complying with its principles.

4. Auditing, Compliance, and Resolution of Non-Compliance

Each unit manager is primarily responsible for taking the necessary measures to ensure compliance with the Information Security Policy and for monitoring the system.

Information Security Management is responsible for periodically auditing compliance with all published policies, procedures, and standards—primarily the Main Information Security Policy—and reporting the findings to the relevant parties.

Violations of the Information Security Policy may cause Ahlatcı Metal Rafineri to suffer damage due to the failure to apply required risk controls. Furthermore, such violations may lead to criminal liability under the Turkish Penal Code and the obligation to compensate for financial damages. Consequently, such an infringement also constitutes a violation of the corporate Personnel Regulations and may result in disciplinary action. Information Security Policy violations detected through supervision, auditing, or reporting may result in internal disciplinary penalties ranging from termination of employment to the initiation of judicial and criminal legal proceedings.

Working together on the implementation of this policy will help ensure the continuous protection of our information and reputation, as well as the continuity of our business success.

5. Objectives

Information Security at Ahlatcı Metal Rafineri aims to protect the institution's reputation, reliability, and information assets, and to ensure that core and supporting business activities continue with minimum interruption. To this end, the objectives are:

- To protect information assets processed, maintained, and shared with other organizations according to the principles of confidentiality, integrity, and availability.

- To manage information assets, determine security values, needs, and risks, and to develop and continuously improve the management system established to implement controls against security risks.
- To determine continuous improvement needs and opportunities by evaluating risks arising from activities in accordance with the corporate vision and mission.
- To follow and adapt to technological developments and changes within the scope of services provided.
- To ensure business continuity by reducing the impact of information security risks.
- To comply with the national and international regulations, legal and legislative requirements, obligations arising from contracts, and corporate responsibilities toward internal and external stakeholders.
- To have the competence to respond quickly to potential information security incidents and minimize their impact.
- To maintain and improve the level of information security over time with a cost-effective control infrastructure.
- To enhance corporate reputation and protect it from negative impacts based on information security.
- To conduct training sessions that improve employees' information security awareness and competencies, and to become an exemplary organization in the sector by providing the necessary support and integrating with other management systems.

Every Ahlatcı Metal Rafineri employee is responsible for contributing to these objectives.

Ahmet Ahlatcı