Arçelik

Information Security Policy: Capital Market Board

1. Information Security Policy Aim and Scope

Information Security Policy aims to identify essential requirements in order to provide accessibility, privacy and integrity of Arçelik information systems and information assets.

Information Security Policy is prepared taking into account the VII-128.9 Information Systems Management Communiqué (Communiqué) enacted by the Capital Markets Board of Turkey for public companies and the Law on the Protection of Personal Data on the subject.

Arçelik has especially adopted the following issues:
- Identifying risks for information assets and managing risks systematically,
- To fulfill the requirements of Information Security Management Standards
- To comply with all legal regulations regarding Information Security,
- Providing the necessary resources for maintaining the Information Security Management System, establishing the controls, evaluating the opportunities for continuous improvement and carrying out the necessary studies for surveillance,
- To provide trainings in a way to develop technical and behavioral competencies in order to increase awareness of information security,

Arçelik provides the establishment and oversight of the controls required to operate and maintain the Information Security Management System processes through sub-policies, procedures and instructions related to this policy.

Information Security Policies, whether full-time, part-time, permanent or contractual, are valid and mandatory for all employees using all information or business systems, regardless of geographic location or business unit. It is obliged that all persons, such as third-party service providers and their affiliated support personnel, who do not fall within these classifications and need access to Arçelik information, adhere to the general principles of this policy and other security responsibilities and obligations to which they must comply.

2. Responsible

Board of Directors and Top Management

To establish an effective information security management structure, the Board of Directors approves the Information Security Policy in which the information security strategy and roadmap are determined and require its implementation. Top Management, consisting of Strategy & Digital Assistant General Manager, Assistant General Manager for Finance & Financial Affairs, Legal and Compliance Director, has been authorized by the Board of Directors to approve all standards, procedures and instructions that must be prepared within the scope of the policy. Senior Management performs the necessary resources and authority / responsibility allocations for the establishment and operation of the Information Security Management System. The Senior Management participates in the Information Security Committee as representative of the Board of Directors, which periodically reviews the information security system. The Senior Management reports to the board member in charge of "Information Security and Cyber Security Management".

All Employees

All employes are obliged to comply with all policies and procedures published under Information Security Management System category, report any security breaches and violations, perform all

The main aim of Information Security and this policy is to protect, maintain and manage the confidentiality, integrity and availability of information and all support business systems, processess and applications which means the information remains in competent responsibles ensuring that information is complete, accurate and available and information is available to systems when needed. Therefore, all Arçelik employees, interns, outsourced employees, dealers, suppliers are required to adhere to Arçelik information security rules.

In this context, asset and process owners are required

- To comply with the Information Security Policy and procedures announced to owners,
- To ensure compliance with Information Security procedures in documents such as process documents, flow diagrams, instructions,

- To report to informationsecurity@arcelik.com in case of any security breaches or in case of non-compliance with Information Security policies and/or procedures
- Not to engage in activities that may adversely affect the operation of information systems or endanger information security.
- To notify the Information Security Manager of the update / improvement requests regarding the Information Security documents.
- Requesting access to information and corporate resources within the scope of business needs.
- To determine the access rights of the owned asset and Personal Data and who can be accessed on an administrator and user basis.
- To observe and update the asset inventory,
- To be responsible for ensuring the classification, updating and review of the assets employees own, including Personal Data.

Arçelik employees are obliged to comply with Arçelik Global Code of Conduct and also employees must protect confidential information specified in Arçelik Personnel Regulation. Arçelik commits to take precautions specified in Personal Data Protection Regulation and comply with Koç Holding Personal Data Protection Regulation.

Third Parties

Arrangements regarding information security that third parties providing goods and services to Arçelik and their employees must comply with are determined through the relevant contracts and security protocols. These include a minimum of the following:

- To act in accordance with Arçelik Policies and Procedures, which regulate the relations with third parties, especially the information security rules reported by contracts or protocols.
- Not sharing the information and assets of Arçelik with others without Arçelik approval and permission
- Using the identities given to them by Arçelik in accordance with contracts and instructions.

- If the employees of the third party working with Arçelik resign or get reassigned, to report this situation to Arçelik within the same day and to ensure that their authorizations are revoked.
- Without Arçelik's permission and approval, not copying any data and software on Arçelik's devices, recording, taking pictures / videos, sharing data / actions that may compromise data security or image without the approval and permission of Arçelik.

Applying system accesses in Arçelik locations under the supervision of Information Technology teams.

3. Policy Ownership and Guidance in Information Security

The functional ownership of this policy and all standards and other supporting documents and training activities will be carried out by IT Security Management and this management will also be a source of advice and guidance regarding the implementation of the policy throughout Arçelik.

IT Security Management will ensure that all employees receive appropriate training to ensure the appropriate level of awareness about Information Security issues and will generally guide the handling of information security incidents. This will ensure that this policy is supported by detailed standards, procedures and processes when necessary, and when they are ready to use as needed. It will also be responsible for ensuring that these policy requirements are passed on to all employees (permanent or periodic) and to all contractor staff. In addition, IT Security Management is also responsible for ensuring that policy requirements are received by all employees, including permanet or periodic and to all contractors.

Top Management will ensure that establishment of a general management framework related to Information Security and this Information Security Policy, ensuring its continuityand up-to-dateness. Top Management will be responsible for the ongoing review of Arçelik and its subsidiaries to ensure that they continue to reflect business requirements or information and changes in the risk environment or threats facing information systems.

Information Security policies are reviewed at least once a year in parallel with the asset and risk updates made to reflect the current risks faced by information assets of Arçelik. Information Security Policies are updated with necessary informations to control new risks and changes in risks. Besides, any Arçelik employee may requrest IT Security Management to change policies for improving them and reflecting the control needs of Arçelik. All requests are evaluated by IT Security Management.

Information Secuirty Policy principles should be applied in line with Arçelik Human Resources Employee Regulations. Employees are also responsible for being aware of and complying with these Information Security Policy principles.

4. Audit and Complying with Policies and Resolution of Non-Compliance

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

IT Security Management is responsible for audits carried out periodically and reporting to relevant parties regarding compliance with all published policies and procedures, especially Information Security Policy.

Information Security Policy violations may cause Arçelik to be harmed as a result of not applying the necessary controls against the risks, and also to result in criminal liability under the new Turkish Penal Code and the liability for damages. Furthermore, these violations are also meant to violate Arçelik Employee Regulation and may result in disciplinary action.

Information Security Policy violations detected as a result of both surveillance, inspection and notice may result in the implementation of internal disciplinary penalties, termination of employment, and even the initiation of Judicial and Criminal legal procedures.

Working together on the implementation of this policy will help to maintain our knowledge and reputation continuously and to ensure the continuity of our business success.

5. Objectives

For the purpose of continuing Arçelik's reputation, reliability, information assets, and basic and supportive business activities with the least possible business interruptions; Arçelik Information Security aims to;

- Fully ensure the continuity of information systems,
- Maximize the level of compliance of employees with awareness, consciuosness and security requirements,
- Ensure full compliance with contracts with third parties.
- Minimize information security violation incidents and converts into opportunities for learning,
- Ensure production, access and storage of information in full compliance with the laws,
- Implement the most current and effective technical security controls.

All employees are responsible for contributing objectives listed in this policy.

Version Date: 27.01.2020