ATHEXGROUP
Athens Exchange Group

Information Security Policy

The Athens Exchange Group recognizes the necessity of protecting the information resources (people, processes, information, and technologies) that are in its possession or under its control as well as the obligation to comply with the Greek and European Legal and Regulatory framework.

The Security Policy applies to all information and information resources of the Group. In addition, it applies to the entire Athens Stock Exchange Group and the individual operating units, including all regional units controlled by it or under it, subsidiaries, external suppliers, and partners. It concerns the creation, processing, communication, distribution, storage, and disposal of both the Group's information and the information of its customers which are made available to the Group for processing, in any way, directly or indirectly, and in any form (digital, written, etc.).

The Security Policy covers current and future activities of the Group as well as relations with executives, employees, customers, partners, project contractors, and subcontractors, who manage – or have access to – information of the Group. It also applies to all bodies, organizations, and companies in the public and private sectors, which provide support, consultancy, and technological or legal services to the Group, whether they operate locally or remotely.

The Security Policy defines the desired level of information security of the Group and sets a set of management, operational, and technological rules which, depending on the degree of risk and the applicable legal and regulatory framework of its operation, determine how the Group protects the information under its responsibility. The Security Policy also defines the role of each person involved in the Organization, including their responsibilities and duties. The Policy aims to formulate the principles and minimum-security requirements for the protection of information, business operations, and related technological information resources used by the Group to achieve its business objectives.

Information Security Policy Statements

ARTICLE 1: Commitment of Management, Staff, and Partners to Compliance with the Security Policy.

ARTICLE 2: Evaluation and Documentation of any Deviation from the Security Policy

ARTICLE 3: Commitment of Staff and Partners to the Acceptable Use of Company Resources.

ARTICLE 4: Secure access to Information Systems based on the minimum necessary rights.

ARTICLE 5: User ID certification for entering the Group's Information Systems.

ARTICLE 6: Implementation of Business Continuity Plans and Procedures.

ARTICLE 7: Ensuring the Availability of Information.

ARTICLE 8: Application of Encryption Mechanisms for High-Level Information Security.

ARTICLE 9: Securing Communication and Exchange of Information via Electronic Mail.

ARTICLE 10: Commitment of Management to Inform Staff About Security Matters.

ARTICLE 11: Commitment of Staff and Partners to Report Security Incidents.

ARTICLE 12: Definition of Owners of Information Resources for all Group Resources.

ARTICLE 13: Classification of Information.

ARTICLE 14: Compliance with the Legal, Regulatory, and Regulatory Framework.

ARTICLE 15: Supervision of Information Systems for smooth and safe operation.

ARTICLE 16: Protection of Information from Malicious Software.

ARTICLE 17: Technological Security Measures for the Protection of the Corporate Network.

ARTICLE 18: Controls for Information Risk Assessment and Management.

ARTICLE 19: Secure Destruction of Information.

ARTICLE 20: Incorporation of Security Measures during the Design and Implementation of new services and products.

ARTICLE 21: Audit and Risk Assessment of Third-Party Information Security.

ARTICLE 22: Control of Information Systems Security Weaknesses

ARTICLE 23: Ensuring Physical Access to the Organization's Facilities and Security of Information Equipment.

ARTICLE 24: Organization of Information Security with separation of powers and responsibilities.