


Document change	Name	INFORMATION SECURITY POLICY	
	Type	POLICY	
	Code	44.POL.01	
	First Approval Date	22/05/2001	
	Revision Approval Date	19/01/2024	
	Revision Number	10	
	Prepared by	INFORMATION SECURITY DIRECTORATE	
	Approved by	BOARD OF MANAGEMENT	

BORSA İSTANBUL A.Ş.

INFORMATION SECURITY POLICY

İSTANBUL – 2024

This document is the property of Borsa İstanbul A.Ş. The current version of the document is available on Borsa İstanbul A.Ş. corporate website. Check that it is the correct version before use.

Contents

1. Revision Records.....	3
1.1 Revision History.....	3
1.2 Comparison Chart.....	4
2. Purpose, Scope and Basis.....	4
2.1 Purpose and Scope.....	4
2.2 Basis	4
3. Definitions and Abbreviations.....	4
4. Roles and Responsibilities.....	5
5. General Content.....	7
5.1 Target Audience	7
5.2 Information Security Organization	7
5.3 Principles of the Information Security Policy.....	7
5.4 Exceptional Circumstances.....	9
6. Miscellaneous and Final Provisions	9
6.1 Repealed Provisions	9
6.2 Enforcement.....	9
6.3 Execution.....	9

1. Revision Records

1.1 Revision History

Rev No:	Revision Date	Revision Points	Revision Explanation
0	22.05.2001		First writing
1	24.12.2010		Update
2	18.07.2012		Update
3	18.04.2013		Update
4	01.01.2016		Update
5	12.12.2018		Update
6	29.09.2020		<p>Headings regarding the Management's Support, Breach and Enforcement of Policy, Review and Update of Information Security Policy are added and changes are made according to the requirements within the scope of ISO/IEC 27001 standard.</p> <p>The responsibilities of the IT Network and Security Directorate are updated and the responsibilities of the Information Security Directorate are added.</p> <p>Additionally, articles numbered 3,4,13,14,16,17,18,19 and 20 are added.</p>
7	29.01.2021		Update
8	18.02.2022		The document is rewritten to ensure the compliance of standards and to make the Information Security Policy more concise and comprehensible.
9	18.10.2022		Within the framework of compliance with standards, the sections on Definitions and Roles and Responsibilities have been updated.
10	19.01.2024		The document MGT Number has been removed from the Revision History table. Stylistic adjustments have been made throughout the document.

1.2 Comparison Chart

- The document MGT Number has been removed from the Revision History table.
- Stylistic adjustments have been made throughout the document.

2. Purpose, Scope and Basis

2.1 Purpose and Scope

This Policy aims to establish structures to protect the information and information assets of Borsa İstanbul A.Ş., to determine the principles of information security to be applied, and to express the support and importance given by the Borsa İstanbul A.Ş. Board of Directors to these efforts and principles.

Defining the information security rules and principles that must be followed to support the strategic plans of Borsa İstanbul A.Ş., to protect the brand value owned, and to comply with relevant legal regulations, as well as identifying the necessary roles and responsibilities for the operation of information security processes, are within the scope of this Policy.

All kinds of information and information assets owned by Borsa İstanbul A.Ş. fall under this Policy, and all activities conducted and processes operated within Borsa İstanbul A.Ş. are carried out in accordance with this Policy.

2.2 Basis

This Policy has been prepared based on the second paragraph of Article 12 of the Articles of Association of Borsa İstanbul A.Ş.

3. Definitions and Abbreviations

Meanings of the terms, expressions and abbreviations used in this Policy are given below;

Board of Directors: Refers to the Board of Directors of the Borsa.

Borsa / Company: Refers to Borsa İstanbul A.Ş.

Business Continuity Management System (BCMS): The management of activities required to ensure the uninterrupted continuation of Borsa business processes within a systematic framework.

Business Partner (İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., Members etc.): Institutions and organizations that have interactive business processes with the Borsa within the framework of mutual agreements.

Business Process: The entire set of operations carried out using resources such as labor, money, materials, technology, etc., to achieve benefits, products, services, information, etc., as a result of fulfilling the duties and responsibilities of the Borsa as defined by relevant regulations.

Information: Refers to all types of data, whether raw or processed, directly produced by Borsa İstanbul A.Ş. or conveyed to it by other institutions or individuals, within the scope of its duties, responsibilities, and activities.

Information Asset: Any hardware, software, or communication infrastructure used for processing, storing, transmitting, protecting, ensuring the continuity, and destroying of produced information.

Information Security: The protection of the following attributes of information assets:

- **Confidentiality:** Ensuring that information is accessible only to authorized users.
- **Integrity:** Ensuring that information cannot be unauthorizedly altered and that any alterations are detectable.
- **Availability:** Ensuring that information is accessible and usable on demand only by authorized users, applications, or systems.

Information Security Control: Measures that can be applied to eliminate or reduce to an acceptable level the vulnerability of information or information assets.

ISD: Refers to the Information Security Directorate.

ISMC: Refers to the Information Security Management Committee.

ISMS (Information Security Management System): A system operated to identify potential information security risks in line with changing technological developments, legal regulations, the organization's internal / external business processes, and the threat landscape, and to implement necessary protection methods for information and information assets.

KVKK: Refers to the Personal Data Protection Law dated 24/03/2016 and numbered 6698.

Unit: Refers to the vice presidencies, directorates, and services established within the framework of the Borsa İstanbul A.Ş. Organization Directive.

User: Refers to all employees of the Borsa and individuals or institutions that are granted access rights to information or information assets owned or in use by the Borsa through contracts or other means.

Supplier: Refers to individuals or institutions that provide services and/or resources needed for the operation of Borsa business processes.

4. Roles and Responsibilities

Board of Directors: Approves the Borsa Information Security Policy with the aim of establishing structures to protect information and information assets and bringing security measures to an appropriate level. It assigns the Information Security Management Committee (ISMC) to monitor the activities required within the framework of this Policy. The Board commits to ensuring the establishment, implementation, effective management, maintenance, integration with Borsa processes, review, improvement, support of Information Security Management System (ISMS) processes within the Company, and providing the necessary resources for this scope.

ISMC: Is responsible for determining information security policies and standards, making decisions necessary for the establishment and operation of the ISMS, ensuring the accessibility of required resources, establishing necessary processes and organizational structure, ensuring that the ISMS objectives are aligned with Company goals, integrating the ISMS with Company processes, monitoring performance to evaluate effectiveness, guiding the Company's information security strategies, ensuring compliance with legal obligations and Borsa regulations, and creating information security control mechanisms. The working principles and procedures of the Committee are defined by the "Borsa İstanbul A.Ş. Information Security Management Committee Directive."

ISD (Information Security Directorate): Is responsible for identifying, implementing, and coordinating appropriate security controls with relevant Borsa units. It is also responsible for reporting information security requirements and activities to the ISMC.

ISMS Senior Management Representative: Is responsible for reporting to the ISMC regarding the operation of the ISMS, managing ISMC meetings, and providing necessary information and guidance to the ISMS Coordinator based on the meeting outcomes. The ISMS Senior Management Representative is the Information Security Director.

ISMS Coordinator: Is responsible for leading the efforts required for the establishment, implementation, maintenance, and continual improvement of the Information Security Management System, coordinating with the designated ISMS Representatives from Borsa units to prepare the Company information assets inventory and conduct Information Security risk assessment studies, ensuring the compliance of ISMS documentation with ISO 27001 standards requirements, and reporting the outcomes of ISMS activities to the Information Security Management Committee, as well as fulfilling other duties included in the ISMS documentation.

ISMS Representatives: Are responsible for working with the ISMS Coordinator to create their own business process information asset inventories, contributing to risk assessment studies as needed, supporting actions identified for detected risks, preparing documentation required by ISO 27001 Standard for their own business processes, informing their supervisor about the ISMS activities they follow and obtaining approval when necessary, informing the ISMS Coordinator about updates and changes related to the ISMS topics they follow, and providing additional information/documents and reports requested by the ISMS Coordinator.

Business Process Owner: Is the person or unit responsible for the operation of the assigned business process in accordance with its purpose, accurately, effectively, and according to current regulations.

Owner of Information: Is the person or unit that produces, procures externally, processes, and makes information available for use. They are obligated to ensure that the information they own is accurate, reliable, current, complete, and understandable. This includes:

- Deciding on the classification of the information,
- Determining information security measures, access, backup, transmission, and destruction requirements with the involvement of relevant stakeholders,
- Reviewing the access rights to the information.

Custodian of Information: Is the person or unit responsible for the storage, protection, and operation (when necessary) of information produced and provided by the owner of the information.

Within the framework of the Information Security Policy, they are obliged to perform the production, processing, distribution, access, and destruction of information in accordance with the information classification determined by the owner, including the controls, and ensure the continuity of these controls.

User: Is obliged to perform their duties related to the protection of information and information assets owned and used by the Borsa against current threats and to act in accordance with the relevant rules.

Business Partner: Is obliged to act within the framework of relevant contracts/agreements to meet the information security requirements of the Borsa.

Supplier: Are individuals or institutions that provide services and/or resources needed for the operation of Borsa business processes. They are obliged to comply with the information security requirements determined by the Borsa.

5. General Content

5.1 Target Audience

The target audience of this Policy includes Borsa employees, business partners, suppliers, and other users who are granted access to information or information assets owned or used by Borsa for any reason.

5.2 Information Security Organization

The implementation and operation of the ISMS across Borsa are conducted under the responsibility of the ISMC. Borsa may decide to establish new committees or dissolve existing ones as deemed necessary.

The necessary controls within the scope of information security are determined in coordination with relevant Borsa units by the ISD, and their implementation is monitored under the responsibility of the ISD.

5.3 Principles of the Information Security Policy

This Policy aims to ensure the uninterrupted continuation of the duties and responsibilities determined for Borsa in accordance with relevant regulations, support Borsa's strategic plans, achieve its vision and mission goals, and protect the information of Borsa, its employees, customers, and business partners by conducting business processes within the framework of the ISMS.

The operation of the ISMS is carried out within the framework of the “information security” rules and principles stated below:

- Borsa ensures compliance with international standards for managing and providing information security, including the principles of the ISO/IEC 27001 Information Security Management System, the Capital Markets Board of Türkiye Communiqué VII-128.9 on Information Systems Management, the KVKK, the Guide on Information and

Communication Security by the Presidency of the Republic of Türkiye Digital Transformation Office, and other legal regulations issued by relevant authorities.

- When determining information security requirements, stakeholder expectations, internal and external factors, and information security issues arising from legislation and contracts are considered. It is essential to apply effective methods to determine and meet the information security requirements of Borsa's business processes in their design and operation. Updating business processes in response to changing environmental effects or information security requirements is the responsibility of the business process owner.
- All information provided to employees or third parties by Borsa, unless otherwise required by legislation or contracts, belongs to Borsa.
- Methods and mechanisms for detecting and preventing information security threats targeting any information or information assets owned by Borsa are implemented. Necessary updates are carried out to ensure these methods and mechanisms provide effective protection against current threats, including planning and implementing necessary investments, projects, and human resources.
- The ISMS is operated with a risk management approach in accordance with the ISO 27001 standard. This approach considers Borsa's information and information assets, the potential losses of confidentiality, integrity, and availability of these assets, and the impact of these losses on Borsa. Managing existing risks with an awareness that it is impossible to eliminate all information security risks completely and that there will always be a "residual risk," and applying corrective and preventive measures effectively to minimize this residual risk is fundamental.
- In the design and operation of Borsa business processes, information security risks are assessed, and controls are established to reduce the likelihood and impact of risks other than those that are accepted or remain. The effective operation of risk assessment activities and controls is the responsibility of the relevant business process owner.
- All information produced, processed, stored, or conveyed by third parties within Borsa is protected by Borsa. The measures that must be adhered to for protecting information assets as required by their sensitivity are determined in the relevant information security legislation.
- For the activities conducted under information security to achieve the intended success, it is essential that users approach the subject with awareness and fulfill their responsibilities.
- To increase the information security awareness of Borsa employees, "Information Security Awareness Training" is organized at least once a year, and employees are supported throughout the year with various awareness activities (announcements, newsletters, posters, awareness assessments, etc.).
- Periodic audits by third parties of the ISMS activities are fundamental. Review and evaluation actions deemed necessary within the scope of audit evaluations are carried out within the framework determined by the ISMC. Results of all audits related to information security activities, whether conducted internally or by external parties, are shared with the ISMC.
- To determine the current status of Borsa information assets against internal and external threats, a penetration test is conducted at least once a year by an expert third party under the coordination of the ISD, and the results and identified action plans are reported to the ISMC. The follow-up of measures included in the action plan approved by the Board of Directors is carried out.
- In collaborations with third parties, they are informed about Borsa information security rules and principles in a manner that includes the provisions specified in the confidentiality

commitment prepared by Borsa, and the necessary documents are added to the contract under the responsibility of the relevant Borsa unit, and a confidentiality commitment is signed by the parties as deemed necessary.

- Being aware of information security, assisting in the implementation of measures related to the security of information, reporting suspicious situations, and supporting business continuity activities required within the ISMS are integral parts of users' job descriptions.
- Users are responsible for protecting the user account information allocated to them on information assets and cannot share this information with third parties. Users are responsible for the actions performed with their allocated user accounts.
- Users must comply with measures established to prevent the loss, corruption, and unauthorized access to the information they access within their authorities. The Custodian of Information is obliged to implement protective and corrective measures.
- Access to physical spaces containing information or information assets owned by Borsa is restricted in a manner consistent with the roles and responsibilities of users. The necessary infrastructure for determining, updating, and securely storing audit logs for verification and authorization methods and mechanisms used in this restriction is established.
- All information security incidents targeting information or information assets owned by Borsa are evaluated within the scope of information security incident management. Following these evaluations, activities to update existing controls or implement new controls are carried out as soon as possible.
- The procedures and principles related to the implementation of this Policy are regulated in the Borsa İstanbul A.Ş. Information Security Procedure.
- This Policy and related documents are reviewed at least once a year by the Information Security Directorate, and necessary improvements are presented to the ISMC.
- To ensure access for all personnel, the policy document and other related documents are made available on the Borsa intranet portal. They are also published on the corporate website for access by external stakeholders.
- This Policy is considered communicated to Borsa employees as of the date it is announced.

5.4 Exceptional Circumstances

Situations that are covered by this Policy but may constitute an exception are conducted with the approval of the ISMC Chair, provided that the rationale is specified in writing by the relevant user or Borsa unit and within the knowledge of the ISD. The ISMC is informed about the matter.

6. Miscellaneous and Final Provisions

6.1 Repealed Provisions

There are no provisions that have been repealed.

6.2 Enforcement

This Policy enters into force on the date of approval by the Board of Directors.

6.3 Execution

The provisions of this Policy are executed by the General Manager.