EFOR YATIRIM SANAYİ TİCARET A.Ş. ("COMPANY")
INFORMATION SECURITY POLICY

1. Scope

This Policy covers the definition of roles and responsibilities required for the operation of information security processes, the establishment of processes for managing risks related to information systems, and the implementation and supervision of controls.

2. Purpose

The purpose of this Policy is to define the requirements necessary to ensure the confidentiality, integrity and availability of the Company's information systems and information assets; and to protect, maintain and manage the confidentiality, integrity and availability of information and all supporting business systems, processes and applications. This means ensuring that information remains in authorized hands, that it is complete, accurate and usable, and that information and systems are available when required.

This Information Security Policy has been prepared in consideration of the Capital Markets Board Communiqué on Information Systems Management (VII-128.9), the TS EN ISO 27001 Standard, the Personal Data Protection Law, and other applicable regulations.

The Company ensures the establishment and supervision of the controls required for the operation and continuity of the Information Security Management System (ISMS) through sub-policies, procedures and instructions aligned with this Policy.

The Company particularly adopts the following principles:

- Managing information assets; determining their security values, requirements and risks; and developing and implementing controls against security risks.
- Defining a framework for identifying information assets, their values, security requirements, vulnerabilities, threats and threat frequencies.
- Defining a framework for assessing the impact of threats on confidentiality, integrity and availability.
- Establishing principles for risk treatment.
- Continuously monitoring risks by reviewing technological expectations within the scope of services provided.
- Fulfilling information security requirements arising from national and international regulations, legal obligations, contractual commitments, and corporate responsibilities toward internal and external stakeholders.
- Reducing the impact of information security threats on service continuity and contributing to continuity.

- Ensuring the capability to respond rapidly to information security incidents and minimize their impact.
- Maintaining and improving the level of information security over time through a cost-effective control infrastructure.
- Enhancing corporate reputation and protecting it against information security-related adverse impacts.
- Ensuring the continuity of the Information Security Management System.
- Supporting all activities aimed at the continuous improvement of the Information Security Management System.

3. Responsibilities

Board of Directors

The Information Security Policy is prepared by Senior Management and approved by the Board of Directors. The Board is responsible for ensuring that effective and adequate controls are established over information systems. The Board authorizes Senior Management to oversee the Policy. Assigned authorities and responsibilities shall be consistent with the segregation of duties principle.

Senior Management

Senior Management is responsible for establishing the overall governance framework for Information Security, ensuring its continuity, and regularly reviewing this Policy to reflect changes in business requirements and the risk environment.

Senior Management oversight includes:

- Annual review and approval of information security policies and responsibilities.
- Identification of potential risks related to information systems and defining mitigation actions.
- Monitoring and annual evaluation of information security incidents.
- Increasing employee awareness through information security training activities.

A qualified Information Systems Security Officer (ISSO) is appointed to ensure the implementation and monitoring of information security controls and to report risks to Senior Management.

A Business Continuity Plan is prepared to ensure the continuity of critical business processes according to risk priorities. Acceptable interruption periods and maximum tolerable data loss are defined within this plan.

Information Systems Security Officer

The ISSO leads the Information Security Management Team (ISMS Team) and is responsible for ensuring compliance with information security procedures, guiding

incident response, maintaining standards and documentation, and communicating policy requirements to employees and contractors.

Other Stakeholders
All employees are required to comply with ISMS policies and procedures, report actual or potential security breaches, and perform their duties in a manner that safeguards Company information.

These obligations apply to all employees and contractors, regardless of employment type or geographic location.

Third Parties
Information security requirements applicable to third parties are defined in relevant contracts and security protocols. Third parties must comply with Company policies, protect Company information assets, and perform system access under IT supervision.

4. Audit and Control
Risk Analysis and Internal Audits are conducted at least annually to reflect current risks faced by Company information assets.

The Company is subject to annual Penetration Tests conducted by independent certified parties, in accordance with the Capital Markets Board Communiqué requirements.

The Company complies with TS EN ISO 27001 requirements and undergoes annual surveillance audits and recertification every three years.

Policy violations may result in disciplinary action, termination of employment, and legal or criminal proceedings.

5. Entry into Force
This Policy enters into force upon approval by the Board of Directors following prior approval of the Early Risk Detection Committee. Any amendments shall become effective upon Board approval and shall be communicated to employees.