PEKER GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.
INFORMATION SECURITY POLICY

1. SCOPE and BASIS

The Information Security Policy ("Policy") covers the information assets of Peker Gayrimenkul Yatırım Ortaklığı A.Ş. ("Company"). It is applied by employees at all locations and suppliers/contractor in and out of the location.

The Information Security Policy has been prepared for publicly traded companies in accordance with the Communiqué on Information Systems Management numbered VII-128.9 ("Communiqué") put into effect by the Capital Markets Board and the Law on the Protection of Personal Data and other regulations.

2. PURPOSE

Peker Gayrimenkul Yatırım Ortaklığı A.Ş. considers corporate knowledge as an extremely valuable asset. The purpose of the Company's Information Security Policy is to prevent information security incidents or minimize the risk of damage by ensuring the confidentiality, integrity and accessibility of information assets to ensure the business continuity of the Company and its subsidiaries and to reduce the impact of potential threats.

In particular, the Company is committed to the fulfillment of the following

- Identifying risks to information assets and manage risks in a systematic manner,
- Fulfilling he requirements of Information Security Standards,
- Complying with all legal regulations related to Information Security,
- Providing the necessary resources for the survival of the Information Security Management System, to establish controls, to evaluate continuous improvement opportunities and to carry out the necessary work for surveillance,
- Conducting trainings to improve technical and behavioral competencies in order to increase information security awareness,

3. INFORMATION SECURITY

Information, like other important business and corporate assets, is an asset that has value to a company and therefore needs to be appropriately protected. Information security protects information from danger and threat areas to ensure business continuity and minimize losses. Information security is defined in the Policy as the protection of the following information qualities:

Confidentiality: Ensuring that the information is only accessible to those authorized to access it

Integrity : Ensuring that information and processing methods are accurate and cannot be altered without authorization

Accessibility: Ensuring that authorized users have the fastest access to information and associated resources when needed

4. AUTHORITY AND RESPONSIBILITY

In order to establish an effective information security management structure, the Board of Directors approves the Information Security Policy, which sets out the information security strategy and roadmap, and requires its implementation.

The preparation, updating and implementation of the Information Security Policy is overseen by the Company's senior management and approved by the Board of Directors. The Company's Board of Directors determines the senior management responsible for this matter. The Company's Board of Directors is responsible for ensuring effective and adequate controls over information systems within the scope of the Information Security Policy.

It is appointed by the Board of Directors from among the senior executives of the Company, consisting of the Senior Management of Information Systems, CFO, Legal and Compliance Unit Manager.

4.1. Duties and Responsibilities of Information Systems Senior Management

i. Establishment, operation and management of information systems,
ii. Regarding the use of Information Systems; preparation of an information security policy to ensure the confidentiality, integrity and accessibility of information when necessary,
iii. Submission of the information security policy to the Board of Directors
iv. Announcement of the information security policy to the staff,
v. Implementation, oversight and control of information security policy
vi. Review and approval of critical projects related to the introduction of new information systems, taking into account the manageability of the associated risks,
vii. Bringing information security measures to the appropriate level and allocating sufficient resources for the activities to be carried out for this purpose,
viii. Annual review and approval of information security policies and all responsibilities,
ix. Performing risk management, which includes identifying potential risks related to information systems and processes together with their impacts and defining activities to mitigate such risks within this framework,
x. Monitoring and annual evaluation of incidents related to information security breaches,
xi. Conducting studies and providing trainings to increase the information security awareness of all employees,
xii. Placing the processes and procedures established for the management of risks related to information systems within the Company's organizational and managerial structure in such a way that they will actually function and carrying out supervision and follow-up regarding their functionality,
xiii. Preparation of a business continuity plan to ensure the continuity of all critical business processes according to risk priorities,
xiv. In order to ensure that the security risks arising from information systems are adequately managed, ensuring the development, operation and updating of controls regarding the measures to ensure the confidentiality, integrity and accessibility of information systems and the data to be processed, transmitted and stored on them, and defining the necessary managerial responsibilities,
xv. Identifying the information assets owned by the Company and those responsible for these assets, creating an inventory of these assets and ensuring that the inventory is up-to-date, classifying information assets according to their importance,
xvi. Ensuring that secure areas are protected with the necessary access controls to ensure that physical

access is only granted to authorized persons,

xvii. Designing and implementing physical protection against damage caused by fire, flood, earthquake, explosion, looting and other natural or man-made disasters,

xviii. Establishing and effectively managing controls to protect networks against threats and to ensure the security of systems, databases and applications using networks,

xix. Taking necessary measures to ensure the integrity of transactions, records and data realized through information systems,

xx. Taking measures to ensure the confidentiality of the transactions realized within the scope of information systems activities and the data transmitted, processed and stored within the scope of these transactions,

xxi. Establishing an effective audit trail recording mechanism for the use of information systems, taking into account the complexity and breadth of the scope of risks, systems or activities on information systems,

xxii. Execution of works and transactions regarding the outsourcing of these services with the approval of the Board of Directors.

4.2. Employee and Third Party Liability

Compliance with the Information Security Policy is applicable and mandatory for all personnel using Company and/or subsidiary information or business systems, whether full-time, part-time, permanent or contractual, regardless of geographical location or business unit. Third party service providers and their affiliated support personnel who do not fall into these classifications and who have access to Company information due to the service they provide must act in accordance with the Policy regulations and obligations.

Those who use the company's IT infrastructure and access information resources:

i. Ensure the confidentiality, integrity and accessibility of the Company's information in personal and electronic communication.

ii. They take security measures determined according to risk levels

iii. They report information security breach incidents to the Information Systems Senior Management and take measures to prevent these breaches.

iv. They do not transmit internal information sources (announcements, documents, etc.) to third parties without authorization.

v. They shall not use the Company's IT resources for activities contrary to the legislation.

vi. Protect the confidentiality, integrity and availability of information belonging to investors, business partners, suppliers or other third parties.

In line with the Information Security Policy, the Company Management (or Information Systems Senior Management) ensures that all employees receive awareness training on information security issues and ensures compliance with the Policy.

5. CONTROL and SURVEILLANCE

Violations of the Information Security Policy may cause damage to the Company as a result of not implementing the necessary controls against risks, as well as legal, administrative and/or criminal liability. Therefore, apart from the control and supervision responsibilities explicitly regulated in the Policy, each unit manager of the Company is also primarily responsible for taking the necessary measures and overseeing the system to ensure compliance with the Information Security Policy.